AN EXPOSITION ON THE KRONECKER-WEBER THEOREM

By

Jason A. Baggett

RECOMMENDED:

Advisory Committee Chair

Chair, Department of Mathematics

APPROVED:

Dean, College of Natural Science and Mathematics

Dean of the Graduate School

Apr 20, 2011

Date

AN EXPOSITION ON THE KRONECKER-WEBER THEOREM

A

THESIS

Presented to the Faculty

of the University of Alaska Fairbanks

in Partial Fulfillment of the Requirements

for the Degree of

MASTER OF SCIENCE

By

Jason A. Baggett, B.S.

Fairbanks, Alaska

May 2011

Abstract

The Kronecker-Weber Theorem is a classification result from Algebraic Number Theory.

Theorem (Kronecker-Weber). *Every finite, abelian extension of* $\mathbb{Q}$ *is contained in a cyclotomic field.*

This result was originally proven by Leopold Kronecker in 1853. However, his proof had some gaps that were later filled by Heinrich Martin Weber in 1886 and David Hilbert in 1896. Hilbert's strategy for the proof eventually led to the creation of the field of mathematics called Class Field Theory, which is the study of finite, abelian extensions of arbitrary fields and is still an area of active research.

Not only is the Kronecker-Weber Theorem surprising, its proof is truly amazing. The idea of the proof is that for a finite, Galois extension K of $\mathbb{Q}$, there is a connection between the Galois group $\mathrm{Gal}(K/\mathbb{Q})$ and how primes of $\mathbb{Z}$ split in a certain subring R of K corresponding to $\mathbb{Z}$ in $\mathbb{Q}$. When $\mathrm{Gal}(K/\mathbb{Q})$ is abelian, this connection is so stringent that the only possibility is that K is contained in a cyclotomic field. In this paper, we give an overview of field/Galois theory and what the Kronecker-Weber Theorem means. We also talk about the ring of integers R of K, how primes split in R, how splitting of primes is related to the Galois group $\mathrm{Gal}(K/\mathbb{Q})$, and finally give a proof of the Kronecker-Weber Theorem using these ideas.

Table of Contents

Page

List of Figures

Acknowledgements

I would like to thank my advisor, Prof. Elizabeth Allman, for working with me these past few years, even when she was out of the country. I would like to the thank the rest of my committee, Profs. John Rhodes and Jill Faudree, for reading and editing my thesis. I would also like to thank my wife, Kristen, for keeping me motivated and listening to me complain. Lastly, I would like to thank my pet turtle, Luna, for keeping me company during so many sleepless nights.

Chapter 1
Introduction

A field extension K of $\mathbb{Q}$ is finite if K is finite dimensional as a $\mathbb{Q}$-vector space; K is abelian if $K/\mathbb{Q}$ is Galois and the Galois group $\mathrm{Gal}(K/\mathbb{Q})$ is abelian. We will define and discuss the Galois group in Chapter 2. A cyclotomic field is a field obtained by adjoining roots of unity to $\mathbb{Q}$. For example, $\mathbb{Q}(\sqrt{2})$ is a finite, abelian extension of $\mathbb{Q}$. Let $\omega_8 = e^{2\pi i/8} = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}$. Then ω_8 is a primitive 8-th root of unity, so $\mathbb{Q}(\omega_8)$ is the 8-th cyclotomic field. Moreover,

$$\omega_8 + \omega_8^7 = \left(\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}\right) + \left(\frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}\right) = \sqrt{2}.$$

Thus, $\sqrt{2} \in \mathbb{Q}(\omega_8)$, and so we must have $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\omega_8)$. This is an example of a more general classification result from Algebraic Number Theory called the Kronecker-Weber Theorem.

Theorem (Kronecker-Weber). *Every finite, abelian extension of* $\mathbb{Q}$ *is contained in a cyclotomic field.*

According to [1], the Kronecker-Weber Theorem was originally proven by Leopold Kronecker in 1853. However, his proof had some gaps in the case when the degree of the extension was a power of 2. The first accepted proof of this result was due to Heinrich Martin Weber in 1886. However, his proof also had a gap when the degree of the extension was 2, although this error went unnoticed for 90 years. The first correct proof was due to David Hilbert in 1896. Hilbert's strategy of the proof eventually led to the field of mathematics called Class Field Theory, which is the study of finite, abelian extensions of arbitrary fields. A problem that is still open in Class Field Theory is Hilbert's Twelfth Problem, a generalization of the Kronecker-Weber Theorem.

Open Problem (Hilbert's Twelfth Problem). *Extend the Kronecker-Weber Theorem to finite, abelian extensions of arbitrary fields.*

Not only is the Kronecker-Weber Theorem surprising, its proof is truly amazing. The idea of the proof is that for a finite, Galois extension K of $\mathbb{Q}$, there is a connection between the Galois group $\mathrm{Gal}(K/\mathbb{Q})$ and how primes of $\mathbb{Z}$ split in a certain subring R of K corresponding to $\mathbb{Z}$ in $\mathbb{Q}$, where splitting of primes in R is an analog of prime factorization for

ideals. When $\mathrm{Gal}(K/\mathbb{Q})$ is abelian, this connection is so stringent that the only possibility is that K is contained in a cyclotomic field. In Chapter 2, we give a short summary of field/Galois theory for the reader to understand the statement of the theorem. In Chapter 3, we define and discuss the properties of this subring R of K corresponding to $\mathbb{Z}$ in $\mathbb{Q}$. In Chapter 4, we discuss what it means for a prime of $\mathbb{Z}$ to split in R. In Chapter 5, we discuss the connection between the Galois group and the splitting of primes. Finally, in Chapter 6, we give a proof of the Kronecker-Weber Theorem.

The proof of the Kronecker-Weber Theorem that I give in this paper comes from a series of exercises in Marcus, [2]. Indeed, almost all of the results in Chapters 3-6 can be found in Marcus, either explicitly or laid out in the exercises. It is difficult to improve on the already great exposition in Marcus, but that is not the intent of this paper. The intent of this paper is in many ways to complement the exposition in Marcus by providing alternative explanations and examples, and by filling in details that he leaves to the reader. Unlike Marcus, my focus will be devoted entirely to proving the Kronecker-Weber Theorem and not to a holistic introduction to Algebraic Number Theory. Because of this, a number of important results and concepts have been downplayed or eliminated all together. Aside from a few major results, the majority of proofs that I include in this paper are for those results derived from exercises in Marcus; in this way, I hope to avoid repeating too much of what Marcus says and simultaneously fill in any details that he omits.

The intended audience for this paper is advanced undergraduate and beginning graduate students who have had at least one semester of graduate level algebra. Ideally, the reader will have had some introduction to Galois theory, but I make no such assumption in this paper. Chapter 2 serves as a brief introduction to field/Galois theory as well as a summary of the important results from these subjects. The exposition that I give in Chapter 2 is partly based off of [3], [4], and from old class notes.

Chapter 3 has several purposes. Firstly, it introduces the reader to the ring of integers of an arbitrary number field K. In regards to the Kronecker-Weber Theorem, the most important points of this chapter are (1) defining the ring of integers (Section 3.1), and (2) that these rings of integers are Dedekind domains, and hence nonzero ideals have a unique factorization into primes (Section 3.5). The second purpose of this chapter is to familiarize the reader with some of the algebraic techniques that will be used, often implicitly, through-

out the rest of the paper. The idea is that the reader sees the results in Chapter 2, and then while working through the proofs in Chapter 3, the reader will begin to see why these results in Chapter 2 are true. Thirdly, this chapter provides a more concrete foundation for the rest of the paper. Very little about the trace, norm, and discriminant actually needs to be said in regard to the Kronecker-Weber Theorem, but these tools are needed for working out examples in later chapters. Lastly, no paper on the Kronecker-Weber Theorem would be complete without including the special case for quadratic extensions of $\mathbb{Q}$. A section of this chapter is devoted to its proof.

Almost all of the results in Chapter 4 can be found in [2]. For this reason, very little is actually proven in this chapter. Instead, the concepts of this chapter are illustrated almost exclusively by examples. One of the few topics in this paper that [2] does a poor job of explaining is the different; Marcus leaves its definition and the proof of all of its important properties to the exercises. However, to include all of the details on the different would be too lengthy, and the reader would gain very little from it. Instead, I merely state the properties that are needed and refer the reader to a great presentation given in [5].

Chapter 5 is probably the most important chapter in this paper. This chapter talks about the connection between Galois theory and Algebraic Number Theory. Despite the fact that all of the proofs in Sections 5.1-5.3 are essentially the same proofs given in [2], I felt that they were important enough to include a second time. Of less importance are the higher ramification groups in Section 5.5, although they receive a disproportionate amount of coverage. The reason for this is that [2] only mentions them and their properties in the exercises.

Finally, in Chapter 6, we get to the purpose of this paper: a proof of the Kronecker-Weber Theorem. Essentially, the proof given here is a rearrangement of the proof given in the exercises of [2]. In [2], the general case is gradually reduced to a very specific case, and the result is proven for this specific case. Although this makes it easier for the reader to follow, the reader is left in the end to retrace the proof to figure out which cyclotomic field the original field is contained in. For this reason and in part to be different from [2] and other presentations of the Kronecker-Weber Theorem, I start with the specific case and build up to the general case. By doing so, in the end we obtain a very specific bound on which cyclotomic field our original field is contained in.

Chapter 2
Field/Galois Theory Summary

2.1 Algebraic Field Extensions

Definition 2.1.1. If K, L are fields and $i : K \hookrightarrow L$ is an embedding, then L is a **field extension** of K. We denote the extension as L/K.

If L/K is an extension of fields, then we may equate $i(K)$ with K. Hence, we will often assume $K \subseteq L$. Moreover, L is a vector space over K. We define the **degree** $[L : K]$ of the extension L/K to be the dimension of L as a K-vector space. If $[L : K] < \infty$, then L is a **finite extension** of K. When L is a finite extension of $\mathbb{Q}$, we say that L is a **number field**. All number fields can be viewed as being contained in $\mathbb{C}$.

Proposition 2.1.2 (Degree is multiplicative in towers/Tower Law)**.** *If $K \subseteq L \subseteq M$ are all fields, then*

$$[M : K] = [M : L][L : K].$$

Proof. If $\{\alpha_1, ..., \alpha_n\}$ is a basis for L over K and $\{\beta_1, ..., \beta_m\}$ is a basis for M over L, then $\{\alpha_1\beta_1, ..., \alpha_n\beta_m\}$ is a basis for M over K. □

Definition 2.1.3. Suppose $K \subseteq L$ for K, L fields and $X \subseteq L$. Then $K(X)$ is the **subfield of L generated by** X, that is, $K(X)$ is the intersection of fields M such that $K \cup X \subseteq M \subseteq L$. Equivalently, $K(X)$ is the field of rational functions in X with coefficients from K. The ring $K[X]$ is the **subring of L generated by** X, and it is the collection of polynomials in X with coefficients from K.

We will be particularly interested in fields L that arise by attaching roots of an irreducible polynomial $f(x)$ over K.

Definition 2.1.4. Suppose $K \subseteq L$ is an extension of fields. Then $\alpha \in L$ **is algebraic over** K if α is a root of a polynomial $f(x) \in K[x]$. We say that L **is algebraic over** K if every element $\alpha \in L$ is algebraic over K.

If $\alpha \in L$ is algebraic over K, then we may find an irreducible polynomial $f(x) \in K[x]$ with α as a root. However, any multiple $kf(x)$ where $k \in K$ is also an irreducible polynomial in $K[x]$ with α as a root. Hence, we may assume that $f(x)$ is monic (has leading coefficient

1). We call such an $f(x)$ the **minimal polynomial** of α over K. If β is also a root of $f(x)$, then β is a **conjugate** of α.

Proposition 2.1.5. *Let L/K be an extension of fields and $\alpha \in L$ be an algebraic element over K. Let $f(x) \in K[x]$ be a monic polynomial with α as a root. Then the following are equivalent and uniquely characterize the minimal polynomial of α:*

(1) $f(x)$ is irreducible.

(2) $f(x)$ divides every polynomial that has α as a root.

(3) $f(x)$ generates the ideal in $K[x]$ of all polynomials that have α as a root.

(4) $\deg(f(x))$ is minimal

Example 2.1.6. We have that $\sqrt{2}$ is algebraic over $\mathbb{Q}$ and has minimal polynomial $x^2 - 2$.

Example 2.1.7. Let $\omega = e^{2\pi i/3}$. Then ω is algebraic over $\mathbb{Q}$ since it is a root of $x^3 - 1$. However, $x^3 - 1$ is not the minimal polynomial of ω since it is reducible over $\mathbb{Q}$: $x^3 - 1 = (x-1)(x^2+x+1)$. Since ω is not a root of $x-1$, ω must be a root of x^2+x+1. Moreover, $x^2 + x + 1$ is irreducible over $\mathbb{Q}$, so $f(x) = x^2 + x + 1$ is the minimal polynomial of ω over $\mathbb{Q}$.

Suppose K is a field and $f(x) \in K[x]$ is irreducible. From intuition from $\mathbb{C}/\mathbb{Q}$, one would believe that there is some field L where $f(x)$ has a root α. Hence, we should be able to talk about roots α of $f(x)$ even though $f(x)$ has no roots in K. This would allow us to talk about $K(\alpha)$ without reference to the larger field L. Indeed, our intuition is correct.

Theorem 2.1.8. *Suppose K is a field and $f(x) \in K[x]$ is an irreducible polynomial. Then there exists a field extension L of K such that $f(x)$ has a root $\alpha \in L$. Moreover, $L = K(\alpha)$ and $[L : K] = \deg(f(x))$. This field L is unique up to isomorphism.*

Proof. The main idea of the proof is to consider the embedding $K \hookrightarrow K[x]/(f(x))$ and that $K[x]/(f(x)) \cong K(\alpha)$. The statement about the degree follows from $\{1, \alpha, ..., \alpha^{n-1}\}$ is a basis for $K(\alpha)$ where $n = \deg(f(x))$. The interested reader may work out the rest of the details. $\square$

Suppose $f(x) \in K[x]$ for K a field. Then a field extension L of K in which $f(x)$ factors completely into linear factors is called **a splitting field** of $f(x)$ over K. The unique (up to isomorphism) smallest splitting field is **the splitting field** of $f(x)$ over K. If $\alpha_1, ..., \alpha_n$ are the roots of $f(x)$ (whose existence is guaranteed by Theorem 2.1.8), then the splitting field of $f(x)$ over K is $K(\alpha_1, ..., \alpha_n)$. More generally, we may define the splitting field of a collection of polynomials $F \subseteq K[x]$ to be the smallest field such that all polynomials in F factor completely. If L is the splitting field of a collection of polynomials over K, then L is called **normal** over K. A field C is **algebraically closed** if every polynomial in $C[x]$ factors completely.

When $f(x) \in \mathbb{Q}[x]$ is irreducible, the roots of $f(x)$ are all distinct from one another. One would hope that this is true for $f(x) \in K[x]$ for arbitrary fields K. However, this is generally false.

Definition 2.1.9. An algebraic element α over K is **separable** if its minimal polynomial over K has distinct roots in its splitting field. An extension of fields L/K is **separable** if every element of L is separable over K. A field K is **perfect** if every algebraic extension L/K is separable.

Note. In this paper, our base field K is always either a subfield of $\mathbb{C}$ (and hence has characteristic 0) or is a finite field. For these fields, K is perfect. In this chapter, we will state all results in full generality and not assume separability. However, in the later chapters and our examples, we will take for granted the fact that all our irreducible polynomials have distinct roots.

One of the main ideas of field theory is that finite extensions are precisely fields which arise from adjoining roots of polynomials.

Theorem 2.1.10. *Suppose L/K is an extension of fields. Then the following are equivalent:*

(1) L is a finite extension of K.

(2) L is a finite, algebraic extension of K.

(3) $L = K(\alpha_1, ..., \alpha_n)$ where α_1 is algebraic over K, α_2 is algebraic over $K(\alpha_1)$, ..., α_n is algebraic over $K(\alpha_1, ..., \alpha_{n-1})$.

(4) $L = K(\alpha_1, ..., \alpha_n)$ *where* $\alpha_1, ..., \alpha_n$ *are algebraic over* K*.*

(5) $L = K[\alpha_1, ..., \alpha_n]$ *where* $\alpha_1, ..., \alpha_n$ *are algebraic over* K*.*

(6) If L *is separable over* K*,* $L = K(\alpha)$ *where* α *is algebraic over* K*.*

Proof. We give a partial sketch of the proof:
(1) $\Rightarrow$ (2) follows since $\{1, \alpha, ..., \alpha^d\}$ is a linearly dependent set for $d = [L : K]$ and all $\alpha \in L$.
(2) $\Rightarrow$ (4) follows by taking $\{\alpha_1, ..., \alpha_n\}$ to be a basis for L over K. Then $L = K(\alpha_1, ..., \alpha_n)$. However, we point out that if $\{\alpha_1, ..., \alpha_n\}$ are generators for L over K, then $\alpha_1, ..., \alpha_n$ need not be a basis for L over K.
(4) $\Rightarrow$ (3) is trivial.
(3) $\Rightarrow$ (1) follows from the multiplicativity of the degree in the tower

$$K \subseteq K(\alpha_1) \subseteq K(\alpha_1, \alpha_2) \subseteq ... \subseteq K(\alpha_1, ..., \alpha_n)$$

and that $[K(\alpha_1, ..., \alpha_{i+1}) : K(\alpha_1, ..., \alpha_i)] = \deg(f(x)) < \infty$ where f is the minimal polynomial of α_{i+1} over $K(\alpha_1, ..., \alpha_i)$.
(4) $\Leftrightarrow$ (5) $K[\alpha_1, ..., \alpha_n]$ is a finite dimensional vector space over K. If $\beta \in K[\alpha_1, ..., \alpha_n]$, then $\{1, \beta, ..., \beta^d\}$ are linearly dependent where $d = \dim_K K[\alpha_1, ..., \alpha_n]$. Write 1 as a linear combination of $\beta, ..., \beta^d$ and factor out β to obtain $1 = \beta g(\beta)$ where $g \in K[x]$. Hence, $K[\alpha_1, ..., \alpha_n]$ is a field.
(6) $\Rightarrow$ (4) is trivial.
(4) $\Rightarrow$ (6) is the Theorem of the Primitive Element from field theory; we will omit its proof. $\square$

Example 2.1.11. Let $K = \mathbb{R}$ and $L = \mathbb{C}$. We have that $[\mathbb{C} : \mathbb{R}] = 2$, so $\mathbb{C}$ is a finite extension of $\mathbb{R}$. Indeed, $\mathbb{C} = \mathbb{R}(i)$ where i has minimal polynomial $f(x) = x^2 + 1$; as predicted by Theorem 2.1.8, $[\mathbb{C} : \mathbb{R}] = 2 = \deg(f(x))$. Moreover, all elements of $\mathbb{C}$ have the form $a + bi$ where $a, b \in \mathbb{R}$; these are polynomials in i with coefficients from $\mathbb{R}$. Hence, $\mathbb{C} = \mathbb{R}[i]$. If $\alpha = a + bi$, then α is a root of $x^2 - 2ax + a^2 + b^2$. Hence, $\mathbb{C}$ is finite and algebraic over $\mathbb{R}$.

2.2 Automorphisms and the Galois Group

Definition 2.2.1. Suppose L/K is an extension of fields. The **Galois group** $\mathrm{Gal}(L/K)$ of L over K is the group of automorphisms σ of L that fix K pointwise (i.e. $\sigma|_K = \mathrm{id}$.)

If $L = K(\alpha_1, ..., \alpha_n)$, then $\sigma \in \mathrm{Gal}(L/K)$ is uniquely determined by its action on the generators $\alpha_1, ..., \alpha_n$. Moreover, it follows immediately from the definition that an automorphism σ of L is a K-linear map if and only if $\sigma \in \mathrm{Gal}(L/K)$.

Suppose $\sigma \in \mathrm{Gal}(L/K)$ and let $f(x) = x^n + a_{n-1}x^{n-1} + ... + a_1x + a_0 \in K[x]$. Then

$$\begin{aligned} f(\sigma(x)) &= (\sigma(x))^n + a_{n-1}(\sigma(x))^{n-1} + ... + a_1(\sigma(x)) + a_0 \\ &= \sigma(x^n) + a_{n-1}\sigma(x^{n-1}) + ... + a_1\sigma(x) + a_0 \\ &= \sigma(x^n) + \sigma(a_{n-1})\sigma(x^{n-1}) + ... + \sigma(a_1)\sigma(x) + \sigma(a_0) \\ &= \sigma(x^n + a_{n-1}x^{n-1} + ... + a_1x + a_0) \\ &= \sigma(f(x)). \end{aligned}$$

In particular, if α is a root of $f(x)$, then $f(\sigma(\alpha)) = \sigma(f(\alpha)) = \sigma(0) = 0$. Hence, $\sigma(\alpha)$ is also a root of $f(x)$. That is, automorphisms of L/K permute roots of polynomials in $K[x]$. If L contains all the roots of $f(x)$ and $f(x)$ is irreducible, then $\mathrm{Gal}(L/K)$ acts transitively on the roots.

Example 2.2.2. Let $L = \mathbb{Q}(\sqrt{2})$ and $K = \mathbb{Q}$. We know that automorphisms of $\mathrm{Gal}(L/K)$ must permute the roots of $x^2 - 2$. We define the automorphisms on the generator and extend to all of L:

$$\sigma_1 : \sqrt{2} \mapsto \sqrt{2} \qquad \sigma_2 : \sqrt{2} \mapsto -\sqrt{2}$$

That is, $\sigma_1(a + b\sqrt{2}) = a + b\sqrt{2}$ and $\sigma_2(a + b\sqrt{2}) = a - b\sqrt{2}$ where $a, b \in \mathbb{Q}$. Then $\mathrm{Gal}(L/K) = \{\sigma_1, \sigma_2\} \cong C_2$ where C_2 is the cyclic group of order 2.

For normal field extensions L/K, we have a nice relationship between automorphisms in $\mathrm{Gal}(L/K)$ and embeddings of $L \hookrightarrow C$ that fix K pointwise where C is an algebraically closed field containing K. For normal extensions, such embeddings when restricted to L are automorphisms of L.

Theorem 2.2.3. *Suppose L/K is an algebraic extension of fields. Then the following are equivalent:*

(1) L is normal over K.

(2) Any polynomial $f(x)$ irreducible over K that has a root in L has all its roots in L.

(3) If $K \subseteq L \subseteq C$ where C is algebraically closed, then every embedding of L into C that fixes K pointwise maps L into L.

(4) If $K \subseteq L \subseteq C$ where C is algebraically closed, then every embedding of L into C that fixes K pointwise comes from an automorphism of L.

Example 2.2.4. Let $L = \mathbb{Q}(\sqrt[3]{2})$ and $K = \mathbb{Q}$. We have that $\sqrt[3]{2}$ has minimal polynomial $x^3 - 2$ over $\mathbb{Q}$, which has other roots $\omega_3\sqrt[3]{2}$ and $\omega_3^2\sqrt[3]{2}$ where $\omega_3 = e^{2\pi i/3}$. Since $\omega_3\sqrt[3]{2} \notin \mathbb{R}$ and $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$, we must have that $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not a normal extension. Indeed, consider the embedding $\sigma : \mathbb{Q}(\sqrt[3]{2}) \hookrightarrow \mathbb{C}$ mapping $\sigma(\sqrt[3]{2}) = \omega_3\sqrt[3]{2}$. This maps $\mathbb{Q}(\sqrt[3]{2}) \to \mathbb{Q}(\omega_3\sqrt[3]{2})$.

Suppose L/K is an algebraic extension that is not normal and that C is algebraically closed. Let $\sigma : L \hookrightarrow C$ be an embedding that fixes K pointwise. Then by adjoining to L all roots of any irreducible polynomial of $K[x]$ that has a root in L, we can find a normal extension M/K with $K \subseteq L \subseteq M$. If σ can be extended to an embedding $\widehat{\sigma} : M \hookrightarrow C$, then $\widehat{\sigma} : M \to M$ is an automorphism of M. That is, if σ can be extended to M, then σ can be extended to an automorphism of M. The next result shows that this can always be done.

Theorem 2.2.5. *Suppose $K \subseteq L \subseteq C$ where L is algebraic over K and C is algebraically closed. Then every embedding $\sigma : K \hookrightarrow C$ extends to an embedding $\sigma : L \hookrightarrow C$. If L/K is finite, then σ extends in at most $[L : K]$ ways, with equality holding if and only if L is separable over K.*

Let L/K be a finite extension and suppose $\sigma \in \mathrm{Gal}(L/K)$. Let C be an algebraically closed field with $K \subseteq L \subseteq C$. Then $\sigma : L \hookrightarrow C$ is an embedding that fixes K pointwise. Moreover, all embeddings of $\sigma : L \hookrightarrow C$ that fix K pointwise come from automorphisms in $\mathrm{Gal}(L/K)$ if and only if L/K is normal. But σ is an extension of the inclusion map $K \hookrightarrow C$. There are at most $[L : K]$ such extensions, with equality if and only if L/K is separable. This shows the following:

Theorem 2.2.6. *Let L be a finite extension of K. Then $|\mathrm{Gal}(L/K)| \leq [L : K]$ with equality holding if and only if L/K is both normal and separable.*

Suppose L/K is an algebraic, normal, and separable extension of fields. Then we say L/K is **Galois**. As it turns out, the Galois group $\mathrm{Gal}(L/K)$ behaves very nicely when L/K is a finite, Galois extension, as we will see in Section 2.5. If L/K is Galois and $\mathrm{Gal}(L/K)$ is abelian, we say that L/K is an **abelian extension**.

2.3 Cyclotomic Fields

For this paper, we will use ω_m and occasionally $\omega(m)$ to denote the primitive m-th root of unity, $e^{2\pi i/m}$.

Definition 2.3.1. The **m-th cyclotomic field** is $\mathbb{Q}(\omega_m)$. The **m-th cyclotomic polynomial** $\Phi_m(x)$ is the minimal polynomial of ω_m over $\mathbb{Q}$.

We have that the m-th roots of unity are precisely the roots of $x^m - 1$. If $d \,\Big|\, m$, then ω_d is an m-th root of unity. By Prop. 2.1.5, $\Phi_d(x)$ divides $x^m - 1$. On the other hand, ω_d is not a root of $x^m - 1$ if d does not divide m. Moreover, using calculus it is easy to see that $x^m - 1$ has no multiple roots. It follows that

$$x^m - 1 = \prod_{d|m} \Phi_d(x).$$

Example 2.3.2. We have that $\omega_4 = i$ has minimal polynomial $\Phi_4(x) = x^2 + 1$ over $\mathbb{Q}$. We have that $1, 2, 4$ are the divisors of 4, and that $\omega_1 = 1$ and $\omega_2 = -1$. This gives us that $\Phi_1(x) = x - 1$ and $\Phi_2(x) = x + 1$. Indeed,

$$x^4 - 1 = (x - 1)(x + 1)(x^2 + 1) = \Phi_1(x)\Phi_2(x)\Phi_4(x).$$

If $k \leq m$ and $(m, k) = 1$, then ω_m^k is also a root of $\Phi_m(x)$. Considering the above factorization of $x^m - 1$, it follows that these are all the roots of $\Phi_m(x)$ and that $\deg(\Phi_m(x)) = \varphi(m)$ where φ is the Euler totient function. Thus, $\mathbb{Q}(\omega_m)$ is the splitting field of the separable polynomial $\Phi_m(x)$, so $\mathbb{Q}(\omega_m)$ is Galois. Theorem 2.1.8 implies that

$$[\mathbb{Q}(\omega_m) : \mathbb{Q}] = \deg(\Phi_m(x)) = \varphi(m).$$

Theorem 2.2.6 implies that $|\,\mathrm{Gal}(\mathbb{Q}(\omega_m)/\mathbb{Q})| = \varphi(m)$. We have that $\phi_k : \omega_m \mapsto \omega_m^k$ where $k \leq m$ and $(m, k) = 1$ generates an automorphism in $\mathrm{Gal}(\mathbb{Q}(\omega_m)/\mathbb{Q})$; since there are $\varphi(m)$ such automorphisms, we obtain that

$$\mathrm{Gal}(\mathbb{Q}(\omega_m)/\mathbb{Q}) = \{\sigma_k \mid \sigma_k : \omega_m \mapsto \omega_m^k \text{ where } k \leq m, (m, k) = 1\}.$$

This gives us a natural isomorphism $\mathrm{Gal}(\mathbb{Q}(\omega_m)/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^*$ via $\sigma_k \mapsto k$.

We can now state the Kronecker-Weber Theorem, whose proof is the goal of this paper.

Theorem (Kronecker-Weber)**.** *Every finite, abelian extension of* $\mathbb{Q}$ *is contained in a cyclotomic field.*

2.4 Finite Fields

Besides subfields of $\mathbb{C}$, the only other fields that will arise in this paper are finite fields. We state some well-known results about finite fields in this section.

Theorem 2.4.1. *If* K *is a finite field of order* q*, then* $q = p^n$ *is a prime power. Conversely, if* $q = p^n$ *is a prime power, then there is a unique field* $\mathbb{F}_q$ *of order* q*. Moreover,* $\mathbb{F}_q$ *is the splitting field of* $f(x) = x^q - x$ *over* $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$*.*

Since $\mathbb{F}_{p^n}$ is the splitting field of $f(x) = x^{p^n} - x$ over $\mathbb{F}_p$, $\mathbb{F}_{p^n}$ is a normal extension of $\mathbb{F}_p$. As we pointed out earlier, $\mathbb{F}_{p^n}$ is separable over $\mathbb{F}_p$. Moreover, $\mathbb{F}_{p^n}$ must have degree n over $\mathbb{F}_p$ by counting elements. Thus, $\mathbb{F}_{p^n}$ is a finite extension of $\mathbb{F}_p$, and hence is algebraic as well. All of this shows that $\mathbb{F}_{p^n}$ is a Galois extension of $\mathbb{F}_p$.

For $\alpha, \beta \in \mathbb{F}_{p^n}$, the identity

$$(\alpha + \beta)^p = \alpha^p + \beta^p$$

always holds true. This follows from the binomial expansion of $(\alpha+\beta)^p$ along with the fact that $\mathbb{F}_{p^n}$ is a field of characteristic p (i.e. $p \cdot 1 = 0$). This identity is sometimes jokingly called the *Freshman's Dream Theorem*. Because of this identity, it follows that the map $\phi : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ defined by

$$\phi(x) = x^p$$

is a field homomorphism. Moreover,

$$\ker(\phi) = \{x \in \mathbb{F}_{p^n} \mid x^p = 0\} = \{0\},$$

so ϕ is injective. Since $\mathbb{F}_{p^n}$ is finite, it follows from the pigeonhole principle that ϕ must also be surjective. Thus, ϕ is an automorphism of $\mathbb{F}_{p^n}$, the **Frobenius automorphism**.

If $x \in \mathbb{Z}$, then Fermat's Little Theorem states that

$$x^p \equiv x \pmod{p}.$$

Consequently, if $x \in \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, then $\phi(x) = x$. Thus, $\phi \in \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$.

We have that for all $\alpha \in \mathbb{F}_{p^n}$ that

$$\phi^k(\alpha) = \alpha^{p^k}.$$

Thus, if the order of ϕ is k, then k is the smallest positive integer so that $\alpha^{p^k} = \phi^k(\alpha) = \alpha$ for all $\alpha \in \mathbb{F}_{p^n}$. But this implies that all $\alpha \in \mathbb{F}_{p^n}$ are roots of $x^{p^k} - x$. Since $x^{p^k} - x$ can have at most p^k roots in $\mathbb{F}_{p^n}$ and there are p^n elements in $\mathbb{F}_{p^n}$, we must have that $k \geq n$. On the other hand, since $\mathbb{F}_{p^n}$ is Galois over $\mathbb{F}_p$, Theorem 2.2.6 implies that

$$|\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)| = [\mathbb{F}_{p^n} : \mathbb{F}_p] = n.$$

Consequently, the order of ϕ must be n, and $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) =< \phi >$. Thus, $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ is cyclic of order n.

2.5 The Galois Correspondence Theorem

Definition 2.5.1. Let L be a field and G be a group of automorphisms of L. Then the **fixed field** L^G is the field of points of L fixed by the action of G.

From Galois theory, we have the following propositions.

Proposition 2.5.2. *Let L be a finite Galois extension of a field K with $G = \mathrm{Gal}(L/K)$. Then $L^G = K$.*

Proposition 2.5.3. *Let L be a field and G be a finite group of automorphisms of L. Let $K = L^G$. Then L is finite Galois over K, $G = \mathrm{Gal}(L/K)$, and $|G| = [L : K]$.*

Now suppose L/K is a Galois extension. Given a subgroup H of the Galois group $\mathrm{Gal}(L/K)$, we have $K \subseteq L^H \subseteq L$ and $H = \mathrm{Gal}(L/L^H)$. On the other hand, given an intermediate field $K \subseteq E \subseteq L$, we have that $H = \mathrm{Gal}(L/E)$ fixes E and hence K as well. Therefore, $H \leq \mathrm{Gal}(L/K)$. This gives a natural correspondence between subgroups of $\mathrm{Gal}(L/K)$ and intermediate fields $K \subseteq E \subseteq L$.

Theorem 2.5.4 (Galois Correspondence Theorem/Fundamental Theorem of Galois Theory). *Let L/K be a finite, Galois extension of fields with $G = \mathrm{Gal}(L/K)$. Let $\mathcal{F}$ be the set*

of intermediate fields, $\mathcal{F} = \{E \text{ a field} \mid K \subseteq E \subseteq L\}$*, and let* $\mathcal{G}$ *be the set of subgroups of* G*. Define the maps* $\gamma : \mathcal{F} \to \mathcal{G}$ *and* $\eta : \mathcal{G} \to \mathcal{F}$ *by*

$$\gamma(E) = \{\sigma \in G \mid \sigma \text{ fixes } E \text{ pointwise}\}$$

and

$$\eta(H) = L^H.$$

Then

1. *The maps* γ *and* η *are inverses and set up a one-to-one correspondence between* $\mathcal{F}$ *and* $\mathcal{G}$ *(the Galois correspondence).*

2. *(inclusion reversing) If* $E_1, E_2 \in \mathcal{F}$ *correspond to* $H_1, H_2 \in \mathcal{G}$*, respectively, then* $E_1 \subseteq E_2$ *if and only if* $H_1 \supseteq H_2$*.*

3. *If* $E \leftrightarrow H$ *for* $E \in \mathcal{F}$ *and* $H \in \mathcal{G}$ *under the Galois correspondence, then* $H = \mathrm{Gal}(L/E)$*,* $|H| = [L : E]$*, and* $[G : H] = [E : K]$*.*

4. *An intermediate field* E *is a normal extension of* K *if and only if* $H = \gamma(E)$ *is a normal subgroup of* G*. In this case,* E *is in fact a Galois extension of* K *and* $\mathrm{Gal}(E/K) \cong G/H$*. More generally, even if* H *is not normal in* G*, the embeddings of* E *into some algebraically closed field* C *that fix* K *pointwise are in one-to-one correspondence with the cosets of* H *in* G*.*

5. *If* $E_1, E_2 \in \mathcal{F}$ *correspond with* $H_1, H_2 \in \mathcal{G}$*, respectively, then* $E_1 \cap E_2 \leftrightarrow < H_1, H_2 >$ *and* $E_1E_2 \leftrightarrow H_1 \cap H_2$*.*

Example 2.5.5. Consider the irreducible polynomial $f(x) = x^4 - 2$ over $\mathbb{Q}$. Then the splitting field of f over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt[4]{2}, i)$. It follows that $\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}$ is Galois. By the tower law,

$$[\mathbb{Q}(\sqrt[4]{2}, i) \ : \ \mathbb{Q}] = [\mathbb{Q}(\sqrt[4]{2}, i) \ : \ \mathbb{Q}(\sqrt[4]{2})][\mathbb{Q}(\sqrt[4]{2}) \ : \ \mathbb{Q}] = 2 \cdot 4 = 8.$$

Hence, $G = \mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q})$ has order 8. Consider the automorphisms

$$\sigma : \begin{cases} \sqrt[4]{2} \mapsto i\sqrt[4]{2} \\ i \mapsto i \end{cases} \qquad \tau : \begin{cases} \sqrt[4]{2} \mapsto \sqrt[4]{2} \\ i \mapsto -i \end{cases}$$

Then $|\sigma| = 4$ and $|\tau| = 2$. Moreover, it is easy to see that $\sigma\tau = \tau\sigma^{-1}$ and that $| < \tau, \sigma > | = 8$. Thus,

$$G =< \tau, \sigma \mid |\tau| = 2, |\sigma| = 4, \sigma\tau = \tau\sigma^{-1} > .$$

From this we deduce that $G \cong D_8$ where D_8 is the dihedral group with 8 elements. Figure 2.1 demonstrates the Galois correspondence between the subgroups of G and the intermediate fields of $\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}$.

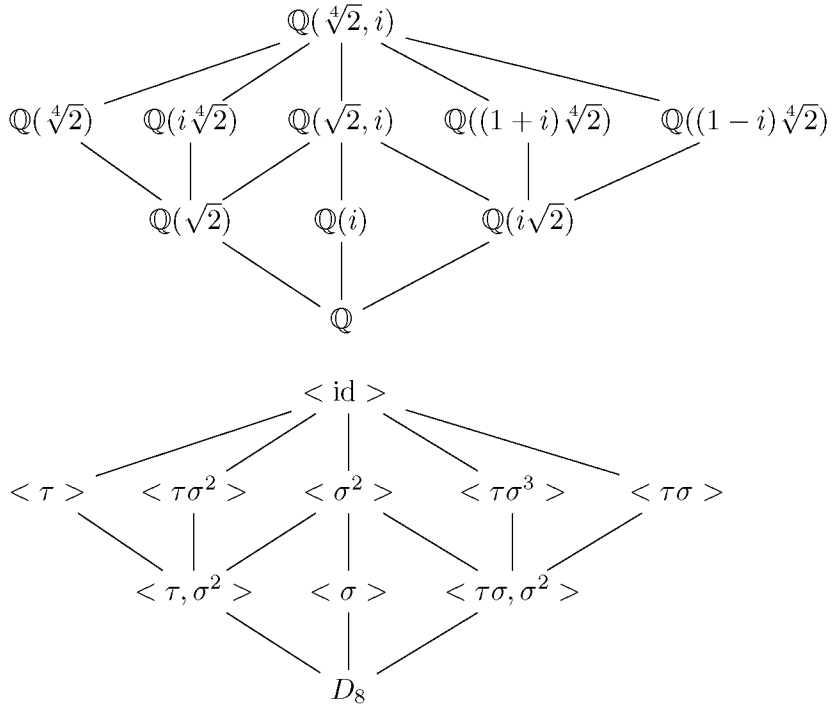


Figure 2.1. The Galois correspondence for $\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}$.

2.6 The Discriminant

The discriminant of the quadratic polynomial $f(x) = x^2 + bx + c$ in $\mathbb{Q}[x]$ is $\Delta = b^2 - 4c$. The discriminant gives a lot information about the nature of the solutions of f. For example, whether Δ is nonnegative or negative tells us respectively whether f has real or nonreal complex roots. We have that $\Delta = 0$ if and only if f has multiple roots. Lastly, $\sqrt{\Delta} \in \mathbb{Q}$ if and only if both roots of f also lie in $\mathbb{Q}$. In this section, we will generalize the discriminant

to any polynomial in $\mathbb{Q}[x]$. As with the quadratic case, the discriminant of a polynomial gives us a lot of information about the roots of the polynomial.

Let K be a field and suppose $f(x) \in K[x]$ is a polynomial of degree n with roots $\alpha_1, ..., \alpha_n$. The **discriminant of** f is

$$\begin{aligned}\Delta(f) &= \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2 \\ &= \begin{vmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \cdots & \alpha_n^{n-1} \end{vmatrix}^2.\end{aligned}$$

Clearly, $f(x)$ is separable over K if and only if $\Delta(f) \neq 0$. Moreover, if L is the splitting field of $f(x)$ over K, then $\sqrt{\Delta(f)} \in L$. Furthermore, if $G = \mathrm{Gal}(L/K)$, then G permutes the roots of $f(x)$. This implies that $\Delta(f)$ is fixed by G, so $\Delta(f) \in L^G$. But $L^G = K$, so $\Delta(f) \in K$.

Example 2.6.1. Let $f(x) = x^2 + bx + c$ over $\mathbb{Q}$. Then the roots of f are $\alpha_1 = \frac{-b+\sqrt{b^2-4c}}{2}$ and $\alpha_2 = \frac{-b-\sqrt{b^2-4c}}{2}$. Then

$$\Delta(f) = (\alpha_1 - \alpha_2)^2 = \left(\sqrt{b^2 - 4c}\right)^2 = b^2 - 4c.$$

This is the usual definition of the discriminant of a quadratic polynomial.

For a polynomial $f(x) \in K[x]$ of degree n and L the splitting field of $f(x)$ over K, we always have that $\mathrm{Gal}(L/K)$ is isomorphic to a subgroup of S_n where S_n is the group of permutations on n elements; as an abuse of language, we will say that $\mathrm{Gal}(L/K) \le S_n$. The discriminant $\Delta(f)$ tells us whether or not $\mathrm{Gal}(L/K) \le A_n$.

Proposition 2.6.2. *Let $f(x) \in K[x]$ be a polynomial of degree n where K is a field of characteristic not equal to 2. Let L be the splitting field of f over K and $G = \mathrm{Gal}(L/K)$. Then $G \le A_n$ if and only if $\sqrt{\Delta(f)} \in K$.*

This result along with the fact that $\Delta(f) = 0$ indicates the presence of multiple roots is one reason for the name discriminant.

Chapter 3
Rings of Algebraic Integers

3.1 Algebraic Integers

Let K be a number field. The goal of this chapter is to derive a subring R that generalizes the subring $\mathbb{Z}$ of $\mathbb{Q}$. We would like R to have K as its field of fractions, $R \cap \mathbb{Q} = \mathbb{Z}$, and for R to have many of the number-theoretic properties that $\mathbb{Z}$ does.

Definition 3.1.1. We say that $\alpha \in \mathbb{C}$ is an **algebraic integer** if α is the root of a monic polynomial with integer coefficients.

Example 3.1.2. The primitive m-th root of unity $\omega_m = e^{2\pi i/m}$ is an algebraic integer since it is a root of $x^m - 1$.

Notice in our definition of an algebraic integer that we do not require the polynomial $f(x) \in \mathbb{Z}[x]$ to be irreducible. However, if α is an algebraic integer, then by factoring into irreducibles we can find an irreducible monic polynomial $f(x) \in \mathbb{Z}[x]$ having α as a root. Thus, α is an algebraic integer if and only if α is the root of a monic irreducible polynomial $f(x) \in \mathbb{Z}[x]$. We will shortly show that in fact α is an algebraic integer if and only if its minimal polynomial $f(x)$ over $\mathbb{Q}$ has coefficients from $\mathbb{Z}$. In order to show this, first we must recall Gauss' Lemma from abstract algebra.

Theorem 3.1.3 (Gauss' Lemma)**.** *Let $f \in \mathbb{Z}[x]$. If f is irreducible in $\mathbb{Z}[x]$, then f is irreducible in $\mathbb{Q}[x]$. Conversely, if the content (the greatest common divisor of the coefficients) of f is 1 and f is irreducible in $\mathbb{Q}[x]$, then f is irreducible in $\mathbb{Z}[x]$.*

Proof. This result and its proof can be found in any abstract algebra textbook. For example, the reader may refer to [3]. □

Proposition 3.1.4. *Let α be an algebraic integer, and let f be the minimal polynomial for α over $\mathbb{Q}$. Then f has coefficients from $\mathbb{Z}$.*

Proof. Since α is an algebraic integer, there is a monic polynomial g with integer coefficients such that α is a root of g. It follows that there is a monic polynomial h with integer coefficients such that α is a root of h and h is irreducible in $\mathbb{Z}[x]$. Since h is monic, the content of h is 1. By Gauss' Lemma, h is irreducible in $\mathbb{Z}[x]$ if and only if h is irreducible

in $\mathbb{Q}[x]$. Thus, h is a monic polynomial that is irreducible in $\mathbb{Q}[x]$ and has α as a root. By the uniqueness of the minimal polynomial, we have that $f = h$. Thus, f has integer coefficients. $\square$

It is generally cumbersome to construct a monic polynomial in $\mathbb{Z}[x]$ having $\alpha \in \mathbb{C}$ as a root in order to show that α is an algebraic integer. The following result gives some equivalent characterizations for being an algebraic integer and mirrors Theorem 2.1.10.

Proposition 3.1.5. *The following are equivalent for $\alpha \in \mathbb{C}$:*

(1) α is an algebraic integer

(2) The ring $\mathbb{Z}[\alpha]$ is a $\mathbb{Z}$-module of finite rank

(3) α is a member of some subring of $\mathbb{C}$ which is a $\mathbb{Z}$-module of finite rank

(4) $\alpha A \subseteq A$ for some finitely-generated nontrivial additive subgroup $A \subseteq \mathbb{C}$

Proof. (1) $\Rightarrow$ (2)
Let $f(x) = x^n + a_{n-1}x^{n-1} + ... + a_1x + a_0$ be the minimal polynomial for α over $\mathbb{Q}$. Then f has integer coefficients by Prop. 3.1.4. We have that

$$\alpha^n = -a_{n-1}\alpha^{n-1} - ... - a_1\alpha - a_0.$$

It follows that for all $k \geq n$, that α^k can be written as a sum of $1, \alpha, ...\alpha^{n-1}$ with integer coefficients. Hence, $\mathbb{Z}[\alpha]$ is generated by $1, \alpha, ..., \alpha^{n-1}$.
(2) $\Rightarrow$ (3) $\Rightarrow$ (4) is immediate
(4) $\Rightarrow$ (1)
Suppose $a_1, ..., a_n$ are generators for A. Expressing αa_i as a linear combination of $a_1, .., a_n$, we obtain

$$\begin{pmatrix} \alpha a_1 \\ \vdots \\ \alpha a_n \end{pmatrix} = M \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$$

where M is an $n \times n$ matrix over $\mathbb{Z}$. That is,

$$M \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = \alpha \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix},$$

Since A is nontrivial, some a_i is nonzero. Hence, α is an eigenvalue of M. Consider the characteristic polynomial of M,

$$f(x) = \det(xI - M).$$

We have that f is a monic polynomial with integer coefficients. Since α is an eigenvalue of M, α is a root of f. Therefore, α is an algebraic integer. □

The previous result allows us to construct algebraic integers in different ways than by taking roots of monic polynomials in $\mathbb{Z}[x]$.

Proposition 3.1.6. *Suppose $a_0, ..., a_{n-1}$ are algebraic integers and α is a root of*

$$x^n + a_{n-1}x^{n-1} + ... + a_1x + a_0.$$

Then α is an algebraic integer.

Proof. Let $d_0, ..., d_{n-1}$ be the respective degrees of $a_0, ..., a_{n-1}$ over $\mathbb{Q}$. Then $\mathbb{Z}[a_0, ..., a_{n-1}, \alpha]$ is generated by the finite set

$$\{a_0^{r_0}...a_{n-1}^{r_{n-1}}\alpha^r \mid 0 \leq r_i \leq d_i - 1, 0 \leq r \leq n-1\}.$$

Thus, $\mathbb{Z}[a_0, ..., a_{n-1}, \alpha]$ is a $\mathbb{Z}$-module of finite rank containing α. By Prop. 3.1.5, α is an algebraic integer. □

Proposition 3.1.7. *If α and β are algebraic integers, then so are $\alpha + \beta$ and $\alpha\beta$.*

Proof. By Prop. 3.1.5, $\mathbb{Z}[\alpha]$ and $\mathbb{Z}[\beta]$ are $\mathbb{Z}$-modules of finite rank. Suppose $\alpha_1, ..., \alpha_m$ are generators for $\mathbb{Z}[\alpha]$ and $\beta_1, ..., \beta_n$ are generators for $\mathbb{Z}[\beta]$. Then

$$\{\alpha_i\beta_j \mid 1 \leq i \leq m, 1 \leq j \leq m\}$$

generates $\mathbb{Z}[\alpha, \beta]$, so $\mathbb{Z}[\alpha, \beta]$ is a $\mathbb{Z}$-module of finite rank. Since $\alpha + \beta$ and $\alpha\beta$ are contained in $\mathbb{Z}[\alpha, \beta]$, it follows from Prop. 3.1.5 that $\alpha + \beta$ and $\alpha\beta$ are algebraic integers. □

It follows immediately that the set of all algebraic integers in a number field K is a ring, which we will denote by $\mathcal{O}_K$. We say that $\mathcal{O}_K$ is a **number ring**, or that $\mathcal{O}_K$ is the **ring of integers** of K. As it turns out, $\mathcal{O}_K$ is the generalization of $\mathbb{Z}$ that we were looking for. One property that we desire is for K to be the field of fractions of $\mathcal{O}_K$. This is indeed true.

Proposition 3.1.8. *For a number field K, K is the field of fractions of $\mathcal{O}_K$.*

Proof. Clearly, the field of fractions of $\mathcal{O}_K$ is contained in K. Let $\alpha \in K$. Then α is a root of a monic polynomial in $\mathbb{Q}[x]$. By clearing denominators, we obtain that α is a root of a polynomial $f(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$ with all $a_i \in \mathbb{Z}$ and $a_n \neq 0$. But then

$$0 = a_n^{n-1} f(\alpha) = (a_n\alpha)^n + a_{n-1}(a_n\alpha)^{n-1} + ... + a_1 a_n^{n-2}(a_n\alpha) + a_0 a_n^{n-1}.$$

Hence, $a_n\alpha$ is a root of the monic polynomial with coefficients from $\mathbb{Z}$

$$g(x) = x^n + a_{n-1}x^{n-1} + ... + a_1 a_n^{n-2} x + a_0 a_n^{n-1}.$$

Thus, $\beta = a_n\alpha$ is an algebraic integer. Therefore, $\alpha = \frac{\beta}{a_n}$ is in the field of fractions of $\mathcal{O}_K$ since $a_n, \beta \in \mathcal{O}_K$. Hence, K is the field of fractions of $\mathcal{O}_K$. □

Example 3.1.9. What is $\mathcal{O}_{\mathbb{Q}}$? These are the rational numbers r whose minimal polynomial over $\mathbb{Q}$ has integer coefficients. But the minimal polynomial of r over $\mathbb{Q}$ is $x - r$. It follows that $r \in \mathbb{Q}$ is an algebraic integer if and only if $r \in \mathbb{Z}$. Hence, $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$.

The previous example and Prop. 3.1.8 show that the ring of integers R of a number field K generalizes $\mathbb{Z}$ in $\mathbb{Q}$. As we will show later on, many properties of $\mathbb{Z}$ also hold for arbitrary number rings.

Example 3.1.10. Let $K = \mathbb{Q}(\sqrt{m})$ where m is a squarefree integer. One might conjecture that $R = \mathcal{O}_K$ is the ring $\mathbb{Z}[\sqrt{m}]$, but this is not generally true. For example, if $m = 5$, then $\alpha = \frac{1+\sqrt{5}}{2}$ is a root of $x^2 - x - 1$, so α is an algebraic integer. Thus, $\alpha \in R$. However, $\alpha \notin \mathbb{Z}[\sqrt{5}]$. In general, $r + s\sqrt{m}$ for $r, s \in \mathbb{Q}$ is a root of $x^2 - 2rx + (r^2 - ms^2)$. Consequently, $r + s\sqrt{m} \in R$ if and only if $2r$ and $r^2 - ms^2$ are both integers. Using elementary number theory, these solutions can be classified. It can be shown that the algebraic integers of K are

$$\mathcal{O}_{\mathbb{Q}(\sqrt{m})} = \begin{cases} \mathbb{Z}[\sqrt{m}] & \text{if } m \equiv 2 \text{ or } 3 \pmod 4 \\ \mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right] & \text{if } m \equiv 1 \pmod 4. \end{cases}$$

More generally, if $K = \mathbb{Q}(\alpha)$ for some algebraic integer α, it is not generally true that $\mathcal{O}_K = \mathbb{Z}[\alpha]$. However, $\mathbb{Z}[\alpha] \subseteq \mathcal{O}_K$ is always true. Determining $\mathcal{O}_K$ for arbitrary number fields K is a difficult question in general. The case for cyclotomic fields is much nicer. We state without proof the following theorem.

Theorem 3.1.11. *$\mathcal{O}_{\mathbb{Q}(\omega_m)} = \mathbb{Z}[\omega_m]$ for all $m \geq 1$.*

3.2 The Trace and Norm

Let K and L be number fields with L an extension of K of degree n. Then there are n embeddings of L into $\mathbb{C}$ that fix K pointwise; denote them $\sigma_1, ..., \sigma_n$. For all $\alpha \in L$, define the **trace** of α in L over K to be

$$T_{L/K}(\alpha) = \sigma_1(\alpha) + ... + \sigma_n(\alpha)$$

and the **norm** of α in L over K to be

$$N_{L/K}(\alpha) = \sigma_1(\alpha)...\sigma_n(\alpha).$$

From the definition, it is easy to see that $T_{L/K}$ is additive and that $N_{L/K}$ is multiplicative since all embeddings σ_i are. Moreover, if $\alpha \in K$, then $T_{L/K}(\alpha) = n\alpha$ and $N_{L/K}(\alpha) = \alpha^n$.

Now suppose $K \subseteq L \subseteq M$ are three number fields. Let $\sigma_1, ..., \sigma_n$ be the embeddings of L into $\mathbb{C}$ fixing K pointwise, and let $\tau_1, ..., \tau_m$ be the embeddings of M into $\mathbb{C}$ fixing L pointwise. By extending these embeddings to automorphisms of a normal extension N of $\mathbb{Q}$ containing M, we obtain that the embeddings of M into $\mathbb{C}$ fixing K pointwise are precisely the maps $\sigma_i\tau_j$ for $1 \leq i \leq n$ and $1 \leq j \leq m$. From this, we easily obtain the following result:

Proposition 3.2.1. *Let K, L, and M be number fields with $K \subseteq L \subseteq M$. Then*

$$T_{M/K} = T_{L/K} \circ T_{M/L}$$
$$N_{M/K} = N_{L/K} \circ N_{M/L}.$$

Suppose $L = K(\alpha)$ and let f be the minimal polynomial for α over K. Then the $\sigma_i(\alpha)$ are precisely the roots of f. Hence, $T_{K(\alpha)/K}(\alpha)$ is the sum of the conjugates of α over K, while $N_{K(\alpha)/K}(\alpha)$ is the product of the conjugates of α over K.

Proposition 3.2.2. *Let L be an extension of K of degree n. Let $\alpha \in L$ and let d be the degree of α over K. Let $t(\alpha)$ and $n(\alpha)$ be the sum and product of the d conjugates of α over K. Then*

$$T_{L/K}(\alpha) = \frac{n}{d}t(\alpha)$$
$$N_{L/K}(\alpha) = n(\alpha)^{n/d}.$$

Proof. Since $d = [K(\alpha) : K]$ and $n = [L : K]$, we have that $n/d = [L : K(\alpha)]$. By our remarks above, we have that $t(\alpha) = T_{K(\alpha)/K}(\alpha)$ and $n(\alpha) = N_{K(\alpha)/K}(\alpha)$. Let f be the minimal polynomial of α over K. Then $-t(\alpha)$ is the coefficient of x^{n-1} in f and $(-1)^d n(\alpha)$ is the constant coefficient in f. Hence, $t(\alpha)$ and $n(\alpha)$ are in K. Thus,

$$\begin{aligned} T_{L/K}(\alpha) &= T_{L/K(\alpha)}(T_{K(\alpha)/K}(\alpha)) \\ &= T_{L/K(\alpha)}(t(\alpha)) \\ &= [L : K(\alpha)]t(\alpha) \\ &= \frac{n}{d}t(\alpha). \end{aligned}$$

Similarly, $N_{L/K}(\alpha) = n(\alpha)^{n/d}$. □

We will often be interested in normal extensions. In this case, the Galois group fixes the ring of integers.

Lemma 3.2.3. *If K and L are number fields with L a normal extension of K, then for each $\alpha \in \mathcal{O}_L$ and each $\sigma \in \mathrm{Gal}(L/K)$, we have that $\sigma(\alpha) \in \mathcal{O}_L$.*

Proof. Let f be the minimal polynomial of α over $\mathbb{Q}$. Since α is an algebraic integer, the coefficients of f must all be integers by Prop. 3.1.4. Since $\mathbb{Q} \subseteq K$, σ fixes $\mathbb{Q}$ pointwise. Thus, $f(\sigma(\alpha)) = \sigma(f(\alpha)) = 0$, so $\sigma(\alpha)$ is a root of f. Hence, $\sigma(\alpha)$ is an algebraic integer. □

In particular if α is an algebraic integer with minimal polynomial f over K, then by taking L to be the splitting field of f we see that all of the conjugates of α are also algebraic integers. Consequently, the trace and norm of an algebraic integer must also be an algebraic integer. Indeed, we can say more than that. Suppose $K \subseteq L$ are number fields and $\alpha \in L$. Let $f(x) = x^d + a_{d-1}x^{d-1} + ... + a_0$ be the minimal polynomial for α over K. Let $\alpha_1, ..., \alpha_d$ be the conjugates of α. Then $\alpha_1, ..., \alpha_d$ are the roots of f, so

$$\begin{aligned} f(x) &= (x - \alpha_1)(x - \alpha_2)...(x - \alpha_d) \\ &= x^d - (\alpha_1 + ... + \alpha_d)x^{d-1} + ... + (-1)^d \alpha_1 ... \alpha_d. \end{aligned}$$

Using the notation of Prop. 3.2.2, this gives us that $t(\alpha) = \alpha_1 + ... + \alpha_d = -a_{d-1}$ and $n(\alpha) = \alpha_1 ... \alpha_d = (-1)^d a_0$. Hence, $t(\alpha), n(\alpha) \in K$. Then Prop. 3.2.2 implies that $T_{L/K}(\alpha), N_{L/K}(\alpha) \in K$. Thus, we have shown the following:

Corollary 3.2.4. *Let K and L be number fields with $K \subseteq L$. For all $\alpha \in L$, $T_{L/K}(\alpha)$ and $N_{L/K}(\alpha)$ are in K. For all $\alpha \in \mathcal{O}_L$, $T_{L/K}(\alpha)$ and $N_{L/K}(\alpha)$ are in $\mathcal{O}_K$.*

In Section 4.5, we will use the trace to define an ideal called the different which tells us about how primes split in number rings. We will use the norm for calculating discriminants in the next section. The norm is also useful for identifying units in a number ring.

Proposition 3.2.5. *Let K be a number field with ring of integers R, and let $\alpha \in R$. Then α is a unit in R if and only if $N_{K/\mathbb{Q}}(\alpha) = \pm 1$.*

Proof. Suppose α is a unit in R. Then $N_{K/\mathbb{Q}}(\alpha)N_{K/\mathbb{Q}}(\alpha^{-1}) = N_{K/\mathbb{Q}}(\alpha\alpha^{-1}) = N_{K/\mathbb{Q}}(1) = 1$. Since $\alpha, \alpha^{-1} \in R$, we have that $N_{K/\mathbb{Q}}(\alpha)$ and $N_{K/\mathbb{Q}}(\alpha^{-1})$ are in $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$ by Corollary 3.2.4. It follows that $N_{K/\mathbb{Q}}(\alpha) = \pm 1$.

Conversely, suppose $N_{K/\mathbb{Q}}(\alpha) = \pm 1$. Let $\alpha = \alpha_1, ..., \alpha_d$ be the conjugates of α and let $n = [K : \mathbb{Q}]$. Then Prop. 3.2.2 implies that $(\alpha_1....\alpha_d)^{n/d} = \pm 1$. This means

$$\alpha_1 \cdot \alpha_1^{(n/d)-1}(\alpha_2...\alpha_d)^{n/d} = \pm 1.$$

By Prop. 3.2.3, we have that all $\alpha_1, ..., \alpha_d$ are algebraic integers since $\alpha = \alpha_1$ is. Therefore, $\alpha_1^{n/d-1}(\alpha_2...\alpha_d)^{n/d}$ is an algebraic integer and up to sign is equal to $\alpha^{-1} \in K$. Thus, α is a unit in R. □

3.3 The Discriminant

In Chapter 2, we discussed the discriminant of a polynomial. We now give some generalizations of the discriminant. In particular, we will eventually give a definition of the discriminant of a number ring. The discriminant of a number ring will have an important property that we will use later on in Chapter 4.

Definition 3.3.1. Let L/K be an extension of number fields with $n = [L : K]$. Let $\sigma_1, ..., \sigma_n$ denote the n embeddings of L into $\mathbb{C}$ that fix K pointwise. For any n-tuple of elements $\alpha_1, ..., \alpha_n \in L$, define the **discriminant of** $\alpha_1, .., \alpha_n$ to be

$$\Delta_{L/K}(\alpha_1, ..., \alpha_n) = \begin{vmatrix} \sigma_1(\alpha_1) & \sigma_1(\alpha_2) & \cdots & \sigma_1(\alpha_n) \\ \sigma_2(\alpha_1) & \sigma_2(\alpha_2) & \cdots & \sigma_2(\alpha_n) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(\alpha_1) & \sigma_n(\alpha_2) & \cdots & \sigma_n(\alpha_n) \end{vmatrix}^2.$$

For $\alpha \in L$, we define $\Delta_{L/K}(\alpha) = \Delta_{L/K}(1, \alpha, ..., \alpha^{n-1})$.

The discriminant of a collection of elements generalizes the discriminant of a polynomial.

Proposition 3.3.2. *Let K be a number field, and let $f(x) \in K[x]$ be a monic irreducible polynomial with root α. Then $\Delta(f) = \Delta_{K(\alpha)/K}(\alpha)$.*

Proof. Let $n = \deg(f(x))$. Then there are n embeddings $\sigma_1, ..., \sigma_n$ of $K(\alpha)$ into $\mathbb{C}$ that fix K pointwise. Moreover, $\alpha_i = \sigma_i(\alpha)$ are the n roots of $f(x)$. Thus, $\sigma_i(\alpha^j) = \alpha_i^j$. Considering the definitions of $\Delta(f)$ and $\Delta_{K(\alpha)/K}(\alpha)$, we obtain that $\Delta(f) = \Delta_{K(\alpha)/K}(\alpha)$. □

Proposition 3.3.3. *Let K and L be number fields with $K \subseteq L$. Let $\alpha_1, ..., \alpha_n \in L$. Then $\Delta_{L/K}(\alpha_1, ..., \alpha_n) = 0$ if and only if $\alpha_1, ..., \alpha_n$ are linearly dependent over K.*

Proof. We have that $\Delta_{L/K}(\alpha_1, ..., \alpha_n) = 0$ if and only if the nullspace of $[\sigma_i(\alpha_j)]$ is nontrivial. That is, there are $a_1, ..., a_n \in K$ not all 0 such that $a_1\sigma_i(\alpha_1) + ...a_n\sigma_i(\alpha_n) = 0$ for all $1 \leq i \leq n$, or equivalently, $\sigma_i(a_1\alpha_1 + ... + a_n\alpha_n) = 0$. Since each σ_i is injective, this is equivalent to $a_1\alpha_1 + ... + a_n\alpha_n = 0$, which is the definition of $\alpha_1, ..., \alpha_n$ being linearly dependent. □

The discriminant is related to the trace and norm, as the next two results demonstrate.

Proposition 3.3.4. *Let L/K be an extension of number fields of degree n. Then for $\alpha_1, ..., \alpha_n \in L$,*

$$\Delta_{L/K}(\alpha_1, ..., \alpha_n) = \begin{vmatrix} T_{L/K}(\alpha_1\alpha_1) & T_{L/K}(\alpha_1\alpha_2) & \cdots & T_{L/K}(\alpha_1\alpha_n) \\ T_{L/K}(\alpha_2\alpha_1) & T_{L/K}(\alpha_2\alpha_2) & \cdots & T_{L/K}(\alpha_2\alpha_n) \\ \vdots & \vdots & \ddots & \vdots \\ T_{L/K}(\alpha_n\alpha_1) & T_{L/K}(\alpha_n\alpha_2) & \cdots & T_{L/K}(\alpha_n\alpha_n) \end{vmatrix}.$$

Proof. Let $\sigma_1, ..., \sigma_n$ be the embeddings of L into $\mathbb{C}$ that fix K pointwise. We have that

$$[\sigma_i(\alpha_j)]^T[\sigma_i(\alpha_j)] = [\sigma_1(\alpha_i\alpha_j) + ... + \sigma_n(\alpha_i\alpha_j)] = [T_{L/K}(\alpha_i\alpha_j)].$$

where i and j are the respective row and column indices. Taking the determinant gives us the desired result. □

It follows that $\Delta_{L/K}(\alpha_1, ..., \alpha_n) \in K$ since each $T_{L/K}(\alpha_i\alpha_j) \in K$. Moreover, if $\alpha_1, ..., \alpha_n \in \mathcal{O}_L$, then $\Delta_{L/K}(\alpha_1, ..., \alpha_n) \in \mathcal{O}_K$.

Proposition 3.3.5. *Let K be a number field and $f(x) \in K[x]$ be a monic irreducible polynomial of degree n with root α. Then*

$$\Delta_{K(\alpha)/K}(\alpha) = \pm N_{K(\alpha)/K}(f'(\alpha))$$

where the $+$ sign holds if and only if $n \equiv 0$ or $1 \pmod 4$.

Proof. Let $\alpha_1, ..., \alpha_n$ denote the roots of f and let $\sigma_1, ..., \sigma_n$ denote the n embeddings of $K(\alpha)$ into $\mathbb{C}$ fixing K pointwise so that $\alpha_i = \sigma_i(\alpha)$. We have that

$$\Delta_{K(\alpha)/K}(\alpha) = \Delta(f) = \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2 = \pm \prod_{i=1}^{n} \prod_{j \neq i} (\alpha_i - \alpha_j),$$

where the $+$ sign holds if and only if $n \equiv 0$ or $1 \pmod 4$. On the other hand,

$$\prod_{i=1}^{n} \prod_{j \neq i} (\alpha_i - \alpha_j) = \prod_{i=1}^{n} f'(\alpha_i) = \prod_{i=1}^{n} f'(\sigma_i(\alpha)) = \prod_{i=1}^{n} \sigma_i(f'(\alpha)) = N_{K(\alpha)/K}(f'(\alpha)).$$

□

First, we defined the discriminant of a polynomial. We then generalized our definition to the discriminant of a set of elements. We will now generalize our definition again to the discriminant of a $\mathbb{Z}$-module. Since number rings are $\mathbb{Z}$-modules, our eventual goal is to define the discriminant of a number ring. However, we can only define the discriminant of a $\mathbb{Z}$-module of the appropriate rank. This will not be a problem, as we will soon see.

Definition 3.3.6. Let K be a number field of degree n over $\mathbb{Q}$. Suppose $M \subseteq K$ is a $\mathbb{Z}$-module of rank n with generators $\alpha_1, ..., \alpha_n$. Then we define the **discriminant of** M to be

$$\Delta(M) = \Delta_{K/\mathbb{Q}}(\alpha_1, ..., \alpha_n).$$

Of course, the above definition requires a choice of basis. Thus, our definition may not be well-defined. We will shortly show that our definition is independent of the choice of basis. In order to do so, we will need the following useful result.

Proposition 3.3.7. *Let K be a number field of degree n over $\mathbb{Q}$. Suppose M, N are two $\mathbb{Z}$-modules of rank n with $N \subseteq M \subseteq K$. Then*

$$\Delta(N) = |M/N|^2 \Delta(M).$$

Proof. Since M and N have the same rank, M/N is finite. Choose $\alpha_1, ..., \alpha_n$ to be generators for M such that $d_1\alpha_1, ..., d_n\alpha_n$ are generators for N for some $d_1, ..., d_n \in \mathbb{N}$. Then $M/N \cong \mathbb{Z}/d_1\mathbb{Z} \oplus ... \oplus \mathbb{Z}/d_n\mathbb{Z}$. Hence, $|M/N| = d_1...d_n$. Let $\sigma_1, ..., \sigma_n$ be distinct embeddings of K into $\mathbb{C}$. Then

$$\begin{aligned}
\Delta(N) &= \begin{vmatrix} d_1\sigma_1(\alpha_1) & d_2\sigma_1(\alpha_2) & \cdots & d_n\sigma_1(\alpha_n) \\ d_1\sigma_2(\alpha_1) & d_2\sigma_2(\alpha_2) & \cdots & d_n\sigma_2(\alpha_n) \\ \vdots & \vdots & \ddots & \vdots \\ d_1\sigma_n(\alpha_1) & d_2\sigma_n(\alpha_2) & \cdots & d_n\sigma_n(\alpha_n) \end{vmatrix}^2 \\
&= (d_1 d_2 ... d_n)^2 \begin{vmatrix} \sigma_1(\alpha_1) & \sigma_1(\alpha_2) & \cdots & \sigma_1(\alpha_n) \\ \sigma_2(\alpha_1) & \sigma_2(\alpha_2) & \cdots & \sigma_2(\alpha_n) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(\alpha_1) & \sigma_n(\alpha_2) & \cdots & \sigma_n(\alpha_n) \end{vmatrix}^2 \\
&= |M/N|^2 \Delta(M).
\end{aligned}$$

□

Corollary 3.3.8. *Let K be a number field of degree n over $\mathbb{Q}$. Let $M \subseteq K$ be a $\mathbb{Z}$-module of rank n. Suppose $\beta_1, ..., \beta_n \in M$. Then M is generated by $\beta_1, ..., \beta_n$ if and only if*

$$\Delta_{K/\mathbb{Q}}(\beta_1, ..., \beta_n) = \Delta(M).$$

It follows that $\Delta(M)$ is well-defined.

Proof. By Prop. 3.3.3, $\Delta(M) \neq 0$. Let $N \subseteq M$ be the $\mathbb{Z}$-module generated by $\beta_1, ..., \beta_n$. If $\Delta_{K/\mathbb{Q}}(\beta_1, ..., \beta_n) = 0$, then $\beta_1, ..., \beta_n$ are linearly dependent over $\mathbb{Q}$ and hence cannot generate M. Hence, we may assume $\Delta(\beta_1, ..., \beta_n) \neq 0$. This means N has rank n, so $\Delta(N) = \Delta_{K/\mathbb{Q}}(\beta_1, ..., \beta_n)$. By Prop. 3.3.7, $\Delta(M) = \Delta(N)$ if and only if $|M/N| = 1$. Hence, $\Delta(M) = \Delta(N)$ if and only if $M = N$. □

Now suppose K is a number field of degree n and $R = \mathcal{O}_K$. Suppose $\{\alpha_1, ..., \alpha_n\} \subseteq R$ is a basis for K over $\mathbb{Q}$. Let M be the $\mathbb{Z}$-module that they generate. It can be shown (see [2]) that

$$M \subseteq R \subseteq \frac{1}{\Delta(M)} M.$$

Since M and $\frac{1}{\Delta(M)} M$ are $\mathbb{Z}$-modules of rank n, it follows that R is a $\mathbb{Z}$-module of rank n.

Proposition 3.3.9. *Let K be a number field of degree n over $\mathbb{Q}$, and let $R = \mathcal{O}_K$. Then R is a $\mathbb{Z}$-module of rank n. Thus, $\Delta(R)$ is well-defined.*

We say that a basis for R over $\mathbb{Z}$ is an **integral basis**. It follows then that an integral basis is also a basis for K over $\mathbb{Q}$. Suppose $\{\alpha_1, ..., \alpha_n\}$ is an integral basis for R. By our earlier remarks following Prop. 3.3.4, $\Delta_{K/\mathbb{Q}}(\alpha_1, ..., \alpha_n) \in \mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$. Thus, $\Delta(R) \in \mathbb{Z}$.

Example 3.3.10. What is the discriminant of $R = \mathcal{O}_{\mathbb{Q}(\sqrt{m})}$ for m a squarefree integer? The embeddings of $K = \mathbb{Q}(\sqrt{m})$ into $\mathbb{C}$ are $\sigma_1 : \sqrt{m} \mapsto \sqrt{m}$ and $\sigma_2 : \sqrt{m} \mapsto -\sqrt{m}$. From Example 3.1.10, we saw that

$$R = \begin{cases} \mathbb{Z}[\sqrt{m}] & \text{if } m \equiv 2 \text{ or } 3 \pmod 4 \\ \mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right] & \text{if } m \equiv 1 \pmod 4. \end{cases}$$

If $m \equiv 2$ or $3 \pmod 4$, then $\{1, \sqrt{m}\}$ is an integral basis for R. Hence,

$$\Delta(R) = \begin{vmatrix} 1 & \sqrt{m} \\ 1 & -\sqrt{m} \end{vmatrix}^2 = 4m.$$

If $m \equiv 1 \pmod 4$, then $\left\{1, \frac{1+\sqrt{m}}{2}\right\}$ is an integral basis for R. Hence,

$$\Delta(R) = \begin{vmatrix} 1 & \frac{1+\sqrt{m}}{2} \\ 1 & \frac{1-\sqrt{m}}{2} \end{vmatrix}^2 = m.$$

Thus,

$$\Delta(\mathcal{O}_{\mathbb{Q}(\sqrt{m})}) = \begin{cases} 4m & \text{if } m \equiv 2 \text{ or } 3 \pmod 4 \\ m & \text{if } m \equiv 1 \pmod 4 \end{cases}.$$

We now turn to finding $\Delta(\mathbb{Z}[\omega_m])$. First, we need the following result:

Proposition 3.3.11. *Let K, L be number fields. Let $R = \mathcal{O}_K$, $S = \mathcal{O}_L$, and $T = \mathcal{O}_{KL}$. Suppose $[KL : \mathbb{Q}] = [K : \mathbb{Q}][L : \mathbb{Q}]$ and $\gcd(\Delta(R), \Delta(S)) = 1$. Then $T = RS$ and*

$$\Delta(T) = \Delta(R)^{[L:\mathbb{Q}]}\Delta(S)^{[K:\mathbb{Q}]}.$$

Example 3.3.12. What is the discriminant of $R = \mathbb{Z}[\omega_m]$? Let $K = \mathbb{Q}(\omega_m)$. First, suppose $m = p$ for p prime. We have that ω_p has minimal polynomial over $\mathbb{Q}$

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = 1 + x + x^2 + ... + x^{p-1}.$$

Differentiating the equation

$$x^p - 1 = (x - 1)\Phi_p(x)$$

gives us

$$px^{p-1} = \Phi_p(x) + (x - 1)\Phi_p'(x).$$

Since $\Phi_p(\omega_p) = 0$, we obtain

$$\Phi_p'(\omega_p) = \frac{p}{\omega_p(\omega_p - 1)}.$$

By Prop. 3.3.5 and the fact that $N_{K/\mathbb{Q}}$ is multiplicative,

$$\Delta(R) = \Delta_{K/\mathbb{Q}}(\omega_p) = N_{K/\mathbb{Q}}\left(\Phi_p'(\omega_p)\right) = \frac{N_{K/\mathbb{Q}}(p)}{N_{K/\mathbb{Q}}(\omega_P)N_{K/\mathbb{Q}}(\omega_p - 1)}.$$

Since $p \in \mathbb{Q}$, $N_{K/\mathbb{Q}}(p) = p^{[K:\mathbb{Q}]} = p^{\varphi(p)} = p^{p-1}$. Using Prop. 3.2.2 and that $\Phi_p(x)$ has constant term 1, we obtain $N_{K/\mathbb{Q}}(\omega_p) = (-1)^{p-1}$. Lastly, suppose $1 \leq l < p$. Then ω_p^l is a root of $\Phi_p(x)$; since there are $\varphi(p) = p - 1 = \deg(\Phi_p(x))$ of them, these are all the roots of $\Phi_p(x)$. Hence,

$$\Phi_p(x) = \prod_{1 \leq l < p} (x - \omega_p^l).$$

This gives us that

$$p = \Phi_p(1) = \prod_{1 \leq l < p} (1 - \omega_p^l).$$

Since all $1 - \omega_p^l$ are conjugates of $1 - \omega_p$, it follows that this product is $N_{K/\mathbb{Q}}(1 - \omega_p)$. Hence, $N_{K/\mathbb{Q}}(1 - \omega_p) = p$. Thus,

$$\Delta(R) = \frac{p^{p-1}}{(-1)^{p-1}(p)} = (-1)^{p-1}p^{p-2}.$$

Next, suppose $m = p^r$ for p prime. We have that ω_{p^r} has minimal polynomial over $\mathbb{Q}$

$$\Phi_{p^r}(x) = \frac{x^{p^r} - 1}{x^{p^{r-1}} - 1} = 1 + x^{p^{r-1}} + x^{2p^{r-1}} + ... + x^{(p-1)p^{r-1}}.$$

Then

$$\begin{aligned}
\Delta_{K/\mathbb{Q}}(\omega_{p^r}) &= \pm N_{K/\mathbb{Q}}(\Phi'_{p^r}(\omega_{p^r})) \\
&= \pm N_{K/\mathbb{Q}}\left(p^{r-1}\omega_{p^r}^{p^{r-1}-1} + 2p^{r-1}\omega_{p^r}^{2p^{r-1}-1} + ... + (p-1)p^{r-1}\omega_{p^r}^{(p-1)p^{r-1}-1}\right) \\
&= \pm N_{K/\mathbb{Q}}\left(p^{r-1}\omega_{p^r}^{-1}\left(\omega_{p^r}^{p^{r-1}} + 2\omega_{p^r}^{2p^{r-1}} + ... + (p-1)\omega_{p^r}^{(p-1)p^{r-1}}\right)\right) \\
&= \pm N_{K/\mathbb{Q}}(p^{r-1})N_{K/\mathbb{Q}}(\omega_{p^r}^{-1})N_{K/\mathbb{Q}}\left(\omega_{p^r}^{p^{r-1}} + 2\omega_{p^r}^{2p^{r-1}} + ... + (p-1)\omega_{p^r}^{(p-1)p^{r-1}}\right)
\end{aligned}$$

with the $+$ if and only if $\varphi(p^r) \equiv 0$ or $1 \pmod 4$. Since $[K : \mathbb{Q}] = \varphi(p^r)$, we have that $N_{K/\mathbb{Q}}(p^{r-1}) = \left(p^{r-1}\right)^{\varphi(p^r)} = p^{(r-1)\varphi(p^r)}$. Moreover, since $N_{K/\mathbb{Q}}$ is multiplicative, we have $N_{K/\mathbb{Q}}(\omega_{p^r}^{-1}) = \frac{1}{N_{K/\mathbb{Q}}(\omega_{p^r})} = 1$ by Prop. 3.2.2. Furthermore,

$$\omega_{p^r}^{p^{r-1}} = \left(e^{2\pi i/p^r}\right)^{p^{r-1}} = e^{2\pi i/p} = \omega_p.$$

Hence,

$$\begin{aligned}
\Delta(R) &= \pm p^{(r-1)\varphi(p^r)} N_{K/\mathbb{Q}}\left(\omega_p + 2\omega_p^2 + ... + (p-1)\omega_p^{p-1}\right) \\
&= \pm p^{(r-1)\varphi(p^r)} N_{K/\mathbb{Q}}(\omega_p) N_{K/\mathbb{Q}}\left(1 + 2\omega_p + ... + (p-1)\omega_p^{p-2}\right) \\
&= \pm p^{(r-1)\varphi(p^r)} N_{K/\mathbb{Q}}(\Phi'_p(\omega_p)) \\
&= \pm p^{(r-1)\varphi(p^r)} N_{\mathbb{Q}(\omega_p)/\mathbb{Q}}\left(N_{K/\mathbb{Q}(\omega_p)}(\Phi'_p(\omega_p))\right) \\
&= \pm p^{(r-1)\varphi(p^r)} N_{\mathbb{Q}(\omega_p)/\mathbb{Q}}\left(\Phi'_p(\omega_p)^{[K:\mathbb{Q}(\omega_p)]}\right) \\
&= \pm p^{(r-1)\varphi(p^r)} N_{\mathbb{Q}(\omega_p)/\mathbb{Q}}(\Phi'_p(\omega_p))^{[K:\mathbb{Q}(\omega_p)]} \\
&= \pm p^{(r-1)\varphi(p^r)} \Delta(\Phi_p)^{[K:\mathbb{Q}(\omega_p)]} \\
&= \pm p^{(r-1)\varphi(p^r)} \left((-1)^{p-1}p^{p-2}\right)^{[K:\mathbb{Q}(\omega_p)]} \\
&= \pm (-1)^{(p-1)[K:\mathbb{Q}(\omega_p)]} p^{(r-1)\varphi(p^r)+(p-2)[K:\mathbb{Q}(\omega_p)]}.
\end{aligned}$$

Since $[K : \mathbb{Q}] = \varphi(p^r)$ and $[\mathbb{Q}(\omega_p) : \mathbb{Q}] = \varphi(p)$, it follows that $[K : \mathbb{Q}(\omega_p)] = \frac{\varphi(p^r)}{\varphi(p)} = p^{r-1}$.

Hence,

$$\begin{aligned}\Delta(R) &= \pm(-1)^{(p-1)p^{r-1}} p^{(r-1)p^{r-1}(p-1)+(p-2)p^{r-1}} \\ &= \pm(-1)^{(p-1)p^{r-1}} p^{r(p-1)p^{r-1}-p^{r-1}} \\ &= \pm(-1)^{(p-1)p^{r-1}} \frac{p^{r(p-1)p^{r-1}}}{p^{p^{r-1}}} \\ &= \pm(-1)^{(p-1)p^{r-1}} \frac{(p^r)^{\varphi(p^r)}}{p^{\varphi(p^r)/(p-1)}}.\end{aligned}$$

Lastly, we consider the general case. Suppose $m = p_1^{r_1} p_2^{r_2} ... p_n^{r_n}$. We have that

$$\mathbb{Q}(\omega_m) = \mathbb{Q}(\omega_{p_1^{r_1}})\mathbb{Q}(\omega_{p_2^{r_2}})...\mathbb{Q}(\omega_{p_n^{r_n}}).$$

Moreover, the above calculation shows that all $\Delta\left(\mathbb{Z}[\omega_{p_i^{r_i}}]\right)$ are relatively prime. Using induction and Prop. 3.3.11, we obtain that

$$\begin{aligned}\Delta(R) &= \Delta\left(\mathbb{Z}[\omega_{p_1^{r_1}}]\right)^{\varphi(m/p_1^{r_1})} \Delta\left(\mathbb{Z}[\omega_{p_2^{r_2}}]\right)^{\varphi(m/p_2^{r_2})} ... \Delta\left(\mathbb{Z}[\omega_{p_n^{r_n}}]\right)^{\varphi(m/p_n^{r_n})} \\ &= \pm \left[\frac{(p_1^{r_1})^{\varphi(p_1^{r_1})}}{p_1^{\varphi(p_1^{r_1})/(p_1-1)}}\right]^{\varphi(m/p_1^{r_1})} ... \left[\frac{(p_n^{r_n})^{\varphi(p_n^{r_n})}}{p_n^{\varphi(p_n^{r_n})/(p_n-1)}}\right]^{\varphi(m/p_n^{r_1})} \\ &= \pm \left[\frac{(p_1^{r_1})^{\varphi(m)}}{p_1^{\varphi(m)/(p_1-1)}}\right] ... \left[\frac{(p_n^{r_n})^{\varphi(m)}}{p_n^{\varphi(m)/(p_n-1)}}\right] \\ &= \pm \frac{m^{\varphi(m)}}{\prod_{\substack{p \text{ prime}, \\ p|m}} p^{\varphi(m)/(p-1)}}.\end{aligned}$$

Lastly, the reader may verify that for $m > 2$ that the $+$ sign holds if and only if $\varphi(m) \equiv 0$ or $1 \pmod 4$. For $m > 2$, this is equivalent to the sign of $(-1)^{\varphi(m)/2}$. Hence, for $m > 2$

$$\Delta(R) = (-1)^{\varphi(m)/2} \frac{m^{\varphi(m)}}{\prod_{\substack{p \text{ prime}, \\ p|m}} p^{\varphi(m)/(p-1)}}.$$

3.4 The Kronecker-Weber Theorem for Quadratic Extensions

We turn now to a simple proof of the Kronecker-Weber Theorem for quadratic extensions $\mathbb{Q}(\sqrt{m})$ where m is a squarefree integer. We have that the quadratic extension $\mathbb{Q}(\sqrt{m})$ is Galois over $\mathbb{Q}$ for all squarefree integers m as it is the splitting field of $x^2 - m$. Moreover, $|\operatorname{Gal}(\mathbb{Q}(\sqrt{m})/\mathbb{Q})| = 2$, so $\operatorname{Gal}(\mathbb{Q}(\sqrt{m})/\mathbb{Q}) \cong C_2$. Hence, all quadratic extensions of $\mathbb{Q}$ are

abelian extensions of $\mathbb{Q}$. We will show that all quadratic extensions of $\mathbb{Q}$ are contained in cyclotomic fields.

Proposition 3.4.1 (Gauss). *Let p be an odd prime. Then $\sqrt{p} \in \mathbb{Q}(\omega_p)$ if $p \equiv 1 \pmod 4$, and $\sqrt{-p} \in \mathbb{Q}(\omega_p)$ if $p \equiv -1 \pmod 4$.*

Proof. We saw in Example 3.3.12 that for p an odd prime $\Delta(\mathbb{Z}[\omega_p]) = \pm p^{p-2}$ with the $+$ if $p \equiv 1 \pmod 4$ and the $-$ if $p \equiv -1 \pmod 4$. But $\Delta(\mathbb{Z}[\omega_p]) = \Delta_{\mathbb{Q}(\omega_p)/\mathbb{Q}}(\omega_p) = \Delta(\Phi_p)$. From the definition of the discriminant of a polynomial, it is easy to see that $\sqrt{\Delta(\Phi_p)} \in \mathbb{Q}(\omega_p)$. But

$$\sqrt{\Delta(\Phi_p)} = \sqrt{\pm p^{p-2}} = \sqrt{\pm p \cdot p^{p-3}} = p^{(p-3)/2}\sqrt{\pm p}.$$

Thus, $p^{(p-3)/2}\sqrt{\pm p} \in \mathbb{Q}(\omega_p)$. Since p is an odd prime, $p^{(p-3)/2} \in \mathbb{Z}$. Consequently, $\sqrt{\pm p} \in \mathbb{Q}(\omega_p)$. □

Corollary 3.4.2. *Let p be an odd prime. Then $\mathbb{Q}(\sqrt{\pm p}) \subseteq \mathbb{Q}(\omega_p)$ with the sign determined by whether $p \equiv \pm 1 \pmod 4$.*

Lemma 3.4.3. *$\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\omega_8)$ and $\mathbb{Q}(i) \subseteq \mathbb{Q}(\omega_8)$.*

Proof. We have that $\omega_8 = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}$. Therefore,

$$\omega_8 + \omega_8^7 = \left(\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}\right) + \left(\frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}\right) = \sqrt{2}.$$

Thus, $\sqrt{2} \in \mathbb{Q}(\omega_8)$, and so we must have $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\omega_8)$. We have that $\mathbb{Q}(i) = \mathbb{Q}(\omega_4) \subseteq \mathbb{Q}(\omega_8)$; in particular, $i = \omega_8^2$. □

Theorem 3.4.4 (Kronecker-Weber Theorem for Quadratic Extensions of $\mathbb{Q}$). *Let m be a squarefree integer and let $d = \Delta(\mathcal{O}_{\mathbb{Q}(\sqrt{m})})$. Then $\mathbb{Q}(\sqrt{m}) \subseteq \mathbb{Q}(\omega_d)$.*

Proof. First, suppose m is odd. Let $m = p_1...p_r$ be its factorization into primes. Since m is squarefree, all p_i are distinct; since m is odd, all p_i are odd. We have that $\sqrt{\pm p_i} \in \mathbb{Q}(\omega_{p_i})$ where $p_i \equiv \pm 1 \pmod 4$. It follows that $\sqrt{\pm m} \in \mathbb{Q}(\omega_{p_1})...\mathbb{Q}(\omega_{p_r}) = \mathbb{Q}(\omega_{p_1...p_r}) = \mathbb{Q}(\omega_m)$ with the sign determined by whether $m \equiv \pm 1 \pmod 4$. Since $i \in \mathbb{Q}(\omega_4)$, we have that $\sqrt{m} = -i\sqrt{-m} \in \mathbb{Q}(i)\mathbb{Q}(\omega_m) = \mathbb{Q}(\omega_{4m})$ when $m \equiv -1 \pmod 4$. Thus, for m odd, $\sqrt{m} \in \mathbb{Q}(\omega_m)$ if $m \equiv 1 \pmod 4$ and $\sqrt{m} \in \mathbb{Q}(\omega_{4m})$ if $m \equiv -1 \pmod 4$. Now suppose m is

even. Then $m/2$ is odd. Regardless of whether $m/2 \equiv \pm 1 \pmod 4$, we always have that $\sqrt{m/2} \in \mathbb{Q}(\omega_{4 \cdot m/2}) = \mathbb{Q}(\omega_{2m})$. Since $\sqrt{2} \in \mathbb{Q}(\omega_8)$, we have that $\sqrt{m} = \sqrt{2}\sqrt{m/2} \in \mathbb{Q}(\omega_8)\mathbb{Q}(\omega_{2m}) \subseteq \mathbb{Q}(\omega_{4m})$ since m is even. In summary,

$$\mathbb{Q}(\sqrt{m}) \subseteq \begin{cases} \mathbb{Q}(\omega_m) & \text{if } m \equiv 1 \pmod 4 \\ \mathbb{Q}(\omega_{4m}) & \text{if } m \equiv 2 \text{ or } 3 \pmod 4 \end{cases}.$$

In Example 3.3.10, we saw that

$$d = \Delta(\mathcal{O}_{\mathbb{Q}(\sqrt{m})}) = \begin{cases} m & \text{if } m \equiv 1 \pmod 4 \\ 4m & \text{if } m \equiv 2 \text{ or } 3 \pmod 4 \end{cases}.$$

Thus, $\mathbb{Q}(\sqrt{m}) \subseteq \mathbb{Q}(\omega_d)$. □

3.5 Dedekind Domains

One might hope that number rings, like $\mathbb{Z}$, are Unique Factorization Domains. However, this is generally false.

Example 3.5.1. Let $K = \mathbb{Q}(\sqrt{-5})$. Then $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. Consider the product

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

We claim that $2, 3, 1 + \sqrt{-5}$, and $1 - \sqrt{-5}$ are all irreducible in $\mathbb{Z}[\sqrt{-5}]$, and so 6 has two distinct factorizations into irreducible elements in $\mathbb{Z}[\sqrt{-5}]$. We have that the embeddings of K into $\mathbb{C}$ are $\sigma_1 : \sqrt{-5} \mapsto \sqrt{-5}$ and $\sigma_2 : \sqrt{-5} \mapsto -\sqrt{-5}$. Hence, for any $a + b\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$, we have that

$$N_{K/\mathbb{Q}}(a + b\sqrt{-5}) = \sigma_1(a + b\sqrt{-5})\sigma_2(a + b\sqrt{-5}) = (a + b\sqrt{-5})(a - b\sqrt{-5}) = a^2 + 5b^2.$$

Since there are no integer solutions a, b to the Diophantine equations $a^2 + 5b^2 = 2$ and $a^2 + 5b^2 = 3$, it follows that no elements of $\mathbb{Z}[\sqrt{-5}]$ have norm 2 or 3. Now $N_{K/\mathbb{Q}}(2) = 4$, $N_{K/\mathbb{Q}}(3) = 9$, $N_{K/\mathbb{Q}}(1+\sqrt{-5}) = 6$, and $N_{K/\mathbb{Q}}(1-\sqrt{-5}) = 6$. Suppose that $2 = \alpha\beta$ for some $\alpha, \beta \in \mathbb{Z}[\sqrt{-5}]$. Then $4 = N_{K/\mathbb{Q}}(2) = N_{K/\mathbb{Q}}(\alpha)N_{K/\mathbb{Q}}(\beta)$. Since $N_{K/\mathbb{Q}}(\alpha)$ and $N_{K/\mathbb{Q}}(\beta)$ are not equal to 2, we must have that (without loss of generality) α has norm 1 and β has norm 4. By Prop. 3.2.5, α is a unit. Thus, 2 is irreducible in $\mathbb{Z}[\sqrt{-5}]$. Similarly, 3, $1 + \sqrt{-5}$, and $1 - \sqrt{-5}$ are irreducible in $\mathbb{Z}[\sqrt{-5}]$. Thus, 6 has two distinct factorizations into irreducible elements, so $\mathbb{Z}[\sqrt{-5}]$ is not a UFD.

Even though elements in a number ring may not factor uniquely into a product of prime elements, as we will see every ideal in a number ring does uniquely factor into a product of prime ideals. This allows many of the proof techniques that work for $\mathbb{Z}$ to carry over to more general number rings.

Definition 3.5.2. A **Dedekind domain** R is an integral domain satisfying the following properties:

(1) R is **Noetherian** — every ideal of R is finitely generated.

(2) Every nonzero prime ideal of R is a maximal ideal.

(3) R is **integrally closed** in its field of fractions K — if $\alpha \in K$ is a root of a monic polynomial over R, then $\alpha \in R$.

We will show that number rings are Dedekind domains. In order to do so, we will need the following result.

Lemma 3.5.3. *Let K be a number field with ring of integers R. Then for any ideal I of R, R/I is finite.*

Theorem 3.5.4. *Every number ring is a Dedekind domain.*

Proof. Let K be a number field of degree n over $\mathbb{Q}$ with ring of integers R. We will show conditions (1)-(3) in Definition 3.5.2 hold.

(1) By Prop. 3.3.9, R has rank n over $\mathbb{Z}$. Since I is a $\mathbb{Z}$-submodule of R, it follows that I must have rank at most n. A basis for I over $\mathbb{Z}$ gives us a set of at most n generators for I. Hence, every ideal in R is finitely generated, so R is Noetherian.

(2) Let P be a nonzero prime ideal of R. Then R/P is a finite integral domain by Lemma 3.5.3, and hence must be a field. Thus, P is a maximal ideal.

(3) We have that the field of fractions of R is K by Prop. 3.1.8. Let $\alpha \in K$ be a root of a monic polynomial over R. Then by Prop. 3.1.6, $\alpha \in R$. Hence, R is integrally closed in its field of fractions K.

□

Similar to $\mathbb{Z}$, we can take products of ideals. Hence, we may say that $A \mid B$ to mean that $B = AC$ for some ideal C. In general, if $A \mid B$, then we must have that $A \supseteq B$. Unlike most rings, the converse is also true for Dedekind domains.

Proposition 3.5.5. *If A and B are ideals in a Dedekind domain R, then $A \mid B$ if and only if $A \supseteq B$.*

Many of the proof techniques from elementary number theory also work for Dedekind domains, except with Dedekind domains the divisibility arguments work for ideals rather than elements. For example, we have a cancellation law for ideals similar to $\mathbb{Z}$.

Proposition 3.5.6 (Cancellation Law)**.** *If $A \neq (0)$, B, and C are ideals in a Dedekind domain and $AB = AC$, then $B = C$.*

These two results allow us to show that ideals in Dedekind domains have a unique factorization into prime ideals.

Theorem 3.5.7. *Every nonzero ideal in a Dedekind domain R is uniquely representable as a product of prime ideals.*

Proof. To show the existence of a prime factorization, suppose to the contrary that not every ideal of R has a prime factorization. Since R is Noetherian, every nonempty set of ideals must have a maximal member. Let M be a maximal member of the set of ideals which have no prime factorization. We have that $M \neq R$ since R is the empty product of prime ideals by convention. Then M is contained in a maximal ideal P of R. Since P is a maximal ideal, P must be a prime ideal of R. By Prop. 3.5.5, $M = PI$ for some ideal I of R. Again, Prop. 3.5.5 implies $M \subseteq I$. If $I = M$, then $RM = M = PI = PM$, so the cancellation law implies $R = P$, which contradicts that P is a maximal ideal. Hence, $M \subsetneq I$. By the maximality of M, we must have that I is a product of primes. But then $M = PI$ is a product of primes, which is a contradiction. Thus, every ideal of R is the product of prime ideals. The proof that the factorization is unique follows from the cancellation law and is similar to the proof of the uniqueness of prime factorizations of integers. □

Since number rings are Dedekind domains, we immediately obtain that the nonzero ideals of a number ring have a unique factorization into prime ideals.

Corollary 3.5.8. *Every nonzero ideal in a number ring R is uniquely representable as a product of prime ideals.*

Because number rings have a unique factorization of nonzero ideals into primes, many of the divisibility arguments from elementary number theory carry over to ideals in number rings.

Example 3.5.9. We have that the ring of integers of $\mathbb{Q}(\sqrt{-6})$ is $R = \mathbb{Z}[\sqrt{-6}]$. How does the principal ideal (5) factor into prime ideals in R? We claim that $(5) = (5, 2+\sqrt{-6})(5, 2-\sqrt{6})$ is the factorization into prime ideals. First we will show that the product on the right is indeed (5). We have that

$$(5, 2 + \sqrt{-6})(5, 2 - \sqrt{6}) = (25, 10 + 5\sqrt{-6}, 10 - 5\sqrt{-6}, 10) = (5)(5, 2 + \sqrt{-6}, 2 - \sqrt{-6}, 2).$$

Since

$$(1) \subseteq (5, 2) \subseteq (5, 2 + \sqrt{-6}, 2 - \sqrt{-6}, 2) \subseteq R = (1),$$

we must have that $(5, 2 + \sqrt{-6}, 2 - \sqrt{-6}, 2) = (1)$. Thus,

$$(5, 2 + \sqrt{-6})(5, 2 - \sqrt{6}) = (5)(5, 2 + \sqrt{-6}, 2 - \sqrt{-6}, 2) = (5)(1) = (5).$$

Next, we must show that $(5, 2 + \sqrt{-6})$ and $(5, 2 - \sqrt{-6})$ are prime ideals. We will show that the quotient rings $\mathbb{Z}[\sqrt{-6}]/(5, 2 + \sqrt{-6})$ and $\mathbb{Z}[\sqrt{-6}]/(5, 2 - \sqrt{-6})$ are in fact fields. To do this, consider the natural ring isomorphism $\mathbb{Z}[\sqrt{-6}] \cong \mathbb{Z}[x]/(x^2 + 6)$ where $\sqrt{-6} \leftrightarrow \overline{x}$ and the bar denotes passage to the quotient. We have that $x^2+6 = (x+2)^2-4(x+2)+2\cdot 5$, so $(x^2 + 6) \subseteq (5, x + 2)$. Therefore, $(5, x + 2)/(x^2 + 6)$ is an ideal of $\mathbb{Z}[x]/(x^2 + 6)$. The ideal $(5, 2+\sqrt{-6})$ in $\mathbb{Z}[\sqrt{-6}]$ corresponds under this isomorphism to the ideal $(5, x+2)/(x^2+6)$ in $\mathbb{Z}[x]/(x^2 + 6)$. Therefore, $\mathbb{Z}[\sqrt{-6}]/(5, 2 + \sqrt{-6}) \cong \frac{\mathbb{Z}[x]/(x^2+6)}{(5,x+2)/(x^2+6)}$. By the Third Isomorphism Theorem, $\frac{\mathbb{Z}[x]/(x^2+6)}{(5,x+2)/(x^2+6)} \cong \mathbb{Z}[x]/(5, x + 2)$. But then

$$\mathbb{Z}[x]/(5, x + 2) \cong (\mathbb{Z}/5\mathbb{Z})[x]/(x + 2) \cong \mathbb{Z}/5\mathbb{Z}.$$

Thus, $\mathbb{Z}[\sqrt{-6}]/(5, 2+\sqrt{-6}) \cong \mathbb{Z}/5\mathbb{Z}$, so $\mathbb{Z}[\sqrt{-6}]/(5, 2+\sqrt{-6})$ is a field. Hence, $(5, 2+\sqrt{-6})$ is a prime ideal. Similarly, $(5, 2 - \sqrt{-6})$ is a prime ideal. Therefore,

$$(5) = (5, 2 + \sqrt{-6})(5, 2 - \sqrt{6})$$

is the factorization of the principal ideal (5) into prime ideals in $\mathbb{Z}[\sqrt{-6}]$.

Example 3.5.10. As we did in Example 3.5.1, let $K = \mathbb{Q}(\sqrt{-5})$. Then $R = \mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. We saw that 6 has two distinct factorizations into irreducible elements in R, namely

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}). \tag{3.1}$$

Proceeding similarly as we did in Example 3.5.9, one can show that prime factorization of the ideal (6) is

$$(6) = (2, 1 + \sqrt{-5})^2(3, 1 + \sqrt{-5})(3, 1 - \sqrt{-5}). \tag{3.2}$$

Letting $I = (2, 1 + \sqrt{-5})$, $J_1 = (3, 1 + \sqrt{-5})$, and $J_2 = (3, 1 - \sqrt{-5})$, notice that $(2) = I^2$, $(3) = J_1J_2$, $(1 + \sqrt{-5}) = IJ_1$, and $(1 - \sqrt{-5}) = IJ_2$. Hence, equation (3.1) is the result of two different rearrangements of equation (3.2)

$$(6) = I^2 \cdot J_1J_2 = IJ_1 \cdot IJ_2.$$

Chapter 4
Splitting of Primes

4.1 Introduction

In this chapter, we will assume that L and K are number fields with $K \subseteq L$. We will denote $R = \mathcal{O}_K$ and $S = \mathcal{O}_L$.

Given a prime ideal P of R, we have that $PS = \{p_1 s_1 + \ldots + p_m s_m \mid p_i \in P, s_i \in S\}$ is an ideal of S containing P. Since S is a Dedekind domain, we have that PS factors uniquely into a product of prime ideals of S. This factorization of PS is called how P **splits** in S (or L). In this chapter, we will focus on how primes split in number rings.

Since R and S are Dedekind domains, we have the following:

Proposition 4.1.1. *Let P be a prime of R and Q be a prime of S. Then the following conditions are equivalent:*

(1) $Q \mid PS$

(2) $Q \supseteq PS$

(3) $Q \supseteq P$

(4) $Q \cap R = P$

(5) $Q \cap K = P$.

If any of the preceding conditions hold, we say that the prime Q **lies over** P and that P **lies under** Q. The primes of S lying over P are precisely the primes which divide PS. That is, they are precisely the primes in the factorization of PS. Since $PS \neq S$, there must be at least one such Q. Hence, P lies under at least one prime of S. On the other hand, given a prime Q of S, it is easy to show that $Q \cap R$ is a prime ideal of R. Hence, every prime Q of S lies over a prime of R, namely $Q \cap R$. Of course, Prop. 4.1.1 shows that this is the only prime that Q may lie over. This establishes the following result:

Proposition 4.1.2. *Every prime Q of S lies over a unique prime P of R; every prime P of R lies under at least one prime Q of S.*

Example 4.1.3. Let $L = \mathbb{Q}(i)$. Then $S = \mathcal{O}_L = \mathbb{Z}[i]$ is a Euclidean Domain, and hence a PID and UFD as well. Suppose p is a prime in $\mathbb{Z}$. How does (p) split in $\mathbb{Z}[i]$? Since $\mathbb{Z}[i]$ is a PID, a factorization $pS = (\alpha_1)^{e_1}...(\alpha_r)^{e_r}$ of the ideal pS corresponds to a factorization of p into irreducible elements: $p = u\alpha_1...\alpha_n$ where u is a unit in $\mathbb{Z}[i]$. Suppose $p = \alpha\beta$ where α and β are not units in $\mathbb{Z}[i]$. Then $p^2 = N_{\mathbb{Q}(i)/\mathbb{Q}}(p) = N_{\mathbb{Q}(i)/\mathbb{Q}}(\alpha)N_{\mathbb{Q}(i)/\mathbb{Q}}(\beta)$. Since α and β are not units, $N_{\mathbb{Q}(i)/\mathbb{Q}}(\alpha)$ and $N_{\mathbb{Q}(i)/\mathbb{Q}}(\beta)$ are not equal to ± 1 by Prop. 3.2.5. Consequently, we must have that $N_{\mathbb{Q}(i)/\mathbb{Q}}(\alpha) = \pm p$ and $N_{\mathbb{Q}(i)/\mathbb{Q}}(\beta) = \pm p$. It is easy to show that if an element of a number ring has prime norm, then that element must be irreducible in that number ring. Hence, α and β must be irreducible.

We have that the embeddings of $\mathbb{Q}(i)$ into $\mathbb{C}$ are $\sigma_1 : i \mapsto i$ and $\sigma_2 : i \mapsto -i$. Hence, for $a + bi \in \mathbb{Z}[i]$, we have that

$$N_{\mathbb{Q}(i)/\mathbb{Q}}(a + bi) = \sigma_1(a + bi)\sigma_2(a + bi) = (a + bi)(a - bi) = a^2 + b^2.$$

Consequently, if p is reducible in $\mathbb{Z}[i]$, then there is a solution $a, b \in \mathbb{Z}$ to $p = a^2 + b^2$. On the other hand, if there is a solution $a, b \in \mathbb{Z}$ to $p = a^2 + b^2$, then $p = (a + bi)(a - bi)$ gives a factorization of p into irreducible elements in $\mathbb{Z}[i]$. Thus, p is reducible in $\mathbb{Z}[i]$ if and only if $p = a^2 + b^2$ for some $a, b \in \mathbb{Z}$. Fermat's Theorem on Sums of Squares from elementary number theory says that a prime p is representable as a sum of two integer squares, $p = a^2 + b^2$, $a, b \in \mathbb{Z}$, if and only if $p = 2$ or $p \equiv 1 \pmod 4$. Consequently, the ideal pS factors into two prime ideals $(a + bi)(a - bi)$ in $\mathbb{Z}[i]$ if and only if $p = 2$ or $p \equiv 1 \pmod 4$. Otherwise, the ideal pS is prime in $\mathbb{Z}[i]$.

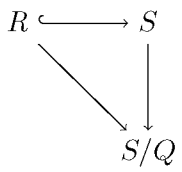
The nonzero prime ideals of $\mathbb{Z}$ are precisely the principal ideals of the form (p) where p is a prime number. In this case, as an abuse of language, we will sometimes say that p is the prime ideal of $\mathbb{Z}$ instead of (p).

4.2 Ramification Indices and Inertial Degrees

Given a prime P of R, there are two natural questions that arise as to how P splits in S. Firstly, we would like to know how many primes of S does P split into and if possible, what those primes are. Secondly, we would like to know the exponents on those primes in the prime factorization of PS. These questions lead us to the following definitions.

Let P be a prime of R, and suppose $PS = Q_1^{e_1}...Q_r^{e_r}$ is the prime factorization of PS in S. We say that the exponents e_i are the **ramification indices** of the Q_i over P, and denote them by $e(Q_i \mid P)$. If $e_i = e(Q_i \mid P) > 1$, then we say that Q_i is **ramified over** P; if $e_i = e(Q_i \mid P) = 1$, then we say that Q_i is **unramified over** P. If some Q_i is ramified over P, then we say that P is **ramified in** S (or L); if all Q_i are unramified over P, then we say that P is **unramified in** S (or L).

We know that the quotient rings R/P and S/Q are fields since P and Q are maximal ideals (recall that nonzero prime ideals are maximal ideals in a Dedekind domain); these are called the **residue fields**. A natural question is how the residue fields R/P and S/Q are related. Consider the natural homomorphism $R \to S/Q$:



The kernel of this homomorphism is $R \cap Q$, which by Prop. 4.1.1 is P. By the First Isomorphism Theorem, we have an embedding $R/P \hookrightarrow S/Q$. Thus, we may view R/P as a subfield of S/Q. Since R/P and S/Q are finite fields, it follows that S/Q must be a Galois extension of R/P. Let f be the degree of the extension. We say that f is the **inertial degree** of Q over P, and we denote it by $f(Q \mid P)$.

Example 4.2.1. Let $L = \mathbb{Q}(\sqrt{-6})$. Then $S = \mathcal{O}_L = \mathbb{Z}[\sqrt{-6}]$. In Example 3.5.9 we saw that the prime factorization of the ideal $5S$ is $(5, 2+\sqrt{-6})(5, 2-\sqrt{6})$. Let $Q_1 = (5, 2+\sqrt{-6})$ and $Q_2 = (5, 2-\sqrt{6})$. Then $e(Q_1 \mid 5) = 1$ and $e(Q_2 \mid 5) = 1$. Thus, Q_1 and Q_2 are unramified over 5, and 5 is unramified in L. Moreover, we saw in that example that $S/Q_1 \cong \mathbb{Z}/5\mathbb{Z}$, so $f(Q_1 \mid 5) = [S/Q_1 : \mathbb{Z}/5\mathbb{Z}] = 1$. Similarly, $S/Q_2 \cong \mathbb{Z}/5\mathbb{Z}$, so $f(Q_2 \mid 5) = 1$.

Proposition 4.2.2 (e and f are multiplicative in towers)**.** *If $P \subseteq Q \subseteq U$ are primes in three number rings $R \subseteq S \subseteq T$, then*

$$e(U \mid P) = e(U \mid Q)e(Q \mid P)$$
$$f(U \mid P) = f(U \mid Q)f(Q \mid P).$$

Proof. The exact power of U dividing Q is $e(U \mid Q)$. The exact power of Q dividing P is $e(Q \mid P)$. It follows that the exact power of U dividing P is $e(U \mid Q)e(Q \mid P)$; by definition, this is $e(U \mid P)$. The fact that f is multiplicative follows from the fact that degrees of field extensions are multiplicative:

$$f(U \mid P) = [T/U : R/P] = [T/U : S/Q][S/Q : R/P] = f(U \mid Q)f(Q \mid P).$$

□

Let I be an ideal of R. Lemma 3.5.3 tells us that R/I is finite. Hence, we may define the **index** of I in R to be

$$\|I\| = |R/I|.$$

We have that S/Q is a finite field of degree $f(Q \mid P)$ over R/P. It follows then that

$$\|Q\| = \|P\|^{f(Q \mid P)}.$$

We list without proof some properties of the index. A proof of these results can be found in [2].

Lemma 4.2.3. *For ideals I and J in a number ring R, we have that*

$$\|IJ\| = \|I\|\|J\|.$$

Lemma 4.2.4. *Let n be the degree of L over K, $R = \mathcal{O}_K$, and $S = \mathcal{O}_L$. Let I be an ideal in R. For the S-ideal IS,*

$$\|IS\| = \|I\|^n.$$

That is, S/IS is an R/I-module of rank n.

The following result is immensely important to us. We have introduced the index solely for its proof.

Theorem 4.2.5. *Let n be the degree of L over K and let $Q_1, ..., Q_r$ be the primes of S lying over a prime P of R. Let $e_1, ..., e_r$ and $f_1, ..., f_r$ denote the corresponding ramification indices and inertial degrees. Then*

$$\sum_{i=1}^{r} e_i f_i = n.$$

Proof. We have that $PS = \prod Q_i^{e_i}$. By Lemma 4.2.3, we have then that

$$\begin{aligned}\|PS\| &= \left\| \prod_{i=1}^{r} Q_i^{e_i} \right\| \\ &= \prod_{i=1}^{r} \|Q_i\|^{e_i} \\ &= \prod_{i=1}^{r} \|P\|^{f_i e_i} \\ &= \|P\|^{\sum_{i=1}^{r} e_i f_i}.\end{aligned}$$

On the other hand, Lemma 4.2.4 gives us that $\|PS\| = \|P\|^n$. Hence, $n = \sum_{i=1}^{r} e_i f_i$. □

Example 4.2.6. Let p be a prime in $\mathbb{Z}$ and let k be a positive integer. How does p split in the p^k-th cyclotomic field $\mathbb{Q}(\omega_{p^k})$? We claim that $p = u(1-\omega_{p^k})^{\varphi(p^k)}$ where u is a unit of $\mathbb{Z}[\omega_{p^k}]$. Let

$$g(x) = \frac{x^{p^k}-1}{x^{p^{k-1}}-1} = 1 + x^{p^{k-1}} + x^{2p^{k-1}} + ... + x^{(p-1)p^{k-1}}.$$

Then the roots of g are precisely the $\omega_{p^k}^l$ where $1 \leq l \leq p^k$ and l not divisible by p since these are the roots of $x^{p^k}-1$ that are not roots of $x^{p^{k-1}}-1$. As an abuse of language, we will say that $l \in (\mathbb{Z}/p^k\mathbb{Z})^*$. Then

$$g(x) = \prod_{l \in (\mathbb{Z}/p^k\mathbb{Z})^*} \left(x - \omega_{p^k}^l\right).$$

Thus, $p = g(1) = \prod_{l \in (\mathbb{Z}/p^k\mathbb{Z})^*} (1-\omega_{p^k}^l)$. Hence,

$$\begin{aligned}p &= \prod_{l \in (\mathbb{Z}/p^k\mathbb{Z})^*} (1-\omega_{p^k}^l) \\ &= \prod_{l \in (\mathbb{Z}/p^k\mathbb{Z})^*} (1-\omega_{p^k})(1+\omega_{p^k}+\omega_{p^k}^2+...+\omega_{p^k}^{l-1}) \\ &= (1-\omega_{p^k})^{\varphi(p^k)} \prod_{l \in (\mathbb{Z}/p^k\mathbb{Z})^*} (1+\omega_{p^k}+\omega_{p^k}^2+...+\omega_{p^k}^{l-1}).\end{aligned}$$

We claim that $u = \prod_{l \in \mathbb{Z}/p^k\mathbb{Z}} (1+\omega_{p^k}+\omega_{p^k}^2+...+\omega_{p^k}^{l-1})$ is a unit in $\mathbb{Z}[\omega_{p^k}]$. Let $l \in (\mathbb{Z}/p^k\mathbb{Z})^*$. Since l is relatively prime to p^k, we have that $hl \equiv 1 \pmod{p^k}$ for some $h \in \mathbb{Z}$. Then $1+\omega_{p^k}+\omega_{p^k}^2+...+\omega_{p^k}^{l-1} = \frac{\omega_{p^k}^l - 1}{\omega_{p^k}-1}$ has inverse $\frac{\omega_{p^k}-1}{\omega_{p^k}^l-1} = \frac{\omega_{p^k}^{hl}-1}{\omega_{p^k}^l-1} \in \mathbb{Z}[\omega_{p^k}]$. Thus, each $1+\omega_{p^k}+\omega_{p^k}^2+...+\omega_{p^k}^{l-1}$ is a unit in $\mathbb{Z}[\omega_{p^k}]$ for $l \in (\mathbb{Z}/p^k\mathbb{Z})^*$, so u is a unit in $\mathbb{Z}[\omega_{p^k}]$ as well.

We have shown that the ideal $(p) = (1-\omega_{p^k})^{\varphi(p^k)}$. Letting Q be a prime dividing $(1-\omega_{p^k})$ and $e = e(Q \mid P)$, we have that $e \geq \varphi(p^k)$. On the other hand, $n = [\mathbb{Q}(\omega_{p^k}) : \mathbb{Q}] = \varphi(p^k)$. By Theorem 4.2.5 and the pigeonhole principle, we must have that $Q = (1-\omega_{p^k})$ is a prime ideal of $\mathbb{Z}[\omega_{p^k}]$, it is the unique prime lying over p, $e(Q \mid p) = \varphi(p^k)$, and $f(Q \mid p) = 1$.

Example 4.2.7. Consider the field $L = \mathbb{Q}(\sqrt[3]{9})$ whose ring of integers $S = \mathcal{O}_L$ is generated by $\left\{1, \sqrt[3]{9}, \frac{(\sqrt[3]{9})^2}{3}\right\}$. How does the prime 61 split in S? We have that the degree of L over $\mathbb{Q}$ is $n = 3$. Moreover, one can verify that

$$61S = (61, \sqrt[3]{9} - 16)(61, \sqrt[3]{9} - 20)(61, \sqrt[3]{9} - 25),$$

and that the ideals $Q_1 = (61, \sqrt[3]{9} - 16)$, $Q_2 = (61, \sqrt[3]{9} - 20)$, and $Q_3 = (61, \sqrt[3]{9} - 25)$ are proper and relatively prime. It follows that the number of primes of S lying over 61 is $r \geq 3$. By Theorem 4.2.5 and the pigeonhole principle, we must have that $r = 3$, Q_1, Q_2, Q_3 are prime ideals of S, and all ramification indices $e_i = e(Q_i \mid 61)$ and inertial degrees $f_i = f(Q_i \mid 61)$ are 1.

Example 4.2.8. As we did in Example 4.1.3, consider the field $L = \mathbb{Q}(i)$ whose ring of integers is $S = \mathbb{Z}[i]$. Then $n = [L : \mathbb{Q}] = 2$. How does the prime (3) split in S? As we showed in Example 4.1.3, a prime (p) of $\mathbb{Z}$ splits into two primes in $\mathbb{Z}[i]$ if and only if $p = 2$ or $p \equiv 1 \pmod 4$; otherwise, (p) remains prime in $\mathbb{Z}[i]$. Since $3 \not\equiv 1 \pmod 4$, we have that (3) remains prime in $\mathbb{Z}[i]$. Thus, there is $r = 1$ prime of S lying over 3 and $e(3S \mid 3) = 1$. Theorem 4.2.5 then implies that $f(3S \mid 3) = 2$.

The previous three examples illustrate the extreme types of behaviour for the splitting of a prime. In Example 4.2.6, we had that there was a unique prime lying over p and its ramification index was n. When $e(Q \mid P) = n = [L : K]$, we say that Q is **totally ramified over** P and that P is **totally ramified in** L. In Example 4.2.7, we had that there were $r = n$ primes lying over 61. When $r = n = [L : K]$, we say that P **splits completely** in L. Lastly, in Example 4.2.8, we had that 3 remained prime in L. When PS is a prime ideal of $S = \mathcal{O}_L$, we say that P is **inert** in L.

As it turns out, if $L = K(\alpha)$ where α has minimal polynomial g over K and P is a prime of R, then the factorization of g in $(R/P)[x]$ gives us the factorization of PS in S for all but finitely many primes P. We will not need this result in our proof of the Kronecker-Weber Theorem; we include this result solely for the purpose of deriving examples.

Theorem 4.2.9. *Let K be a number field, $L = K(\alpha)$, $n = [L : K]$, $R = \mathcal{O}_K$, $S = \mathcal{O}_L$, and g be the minimal polynomial for α over K. Let P be a prime of R and let $(p) = P \cap \mathbb{Z}$. Letting bars denote the passage to the quotient $(R/P)[x]$, suppose $\overline{g} = \overline{g_1}^{e_1}...\overline{g_r}^{e_r}$ is the factorization of $\overline{g}$ into irreducibles in $(R/P)[x]$. If p does not divide $|S/R[\alpha]|$, then*

$$PS = Q_1^{e_1}...Q_r^{e_r}$$

is the prime decomposition of PS where

$$Q_i = PS + (g_i(\alpha)).$$

Moreover, $f(Q_i \mid P) = \deg(g_i)$.

Example 4.2.10. Let $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Then L has degree 4 over $\mathbb{Q}$. We have that L has ring of integers $S = \mathcal{O}_L$ is the $\mathbb{Z}$-module generated by $\left\{1, \sqrt{3}, \sqrt{2}, \frac{\sqrt{2}+\sqrt{6}}{2}\right\}$. How does 3 split in L?

We would like to use Theorem 4.2.9, but in order to do so, we first need to find a single generator for L over K. We claim that $L = \mathbb{Q}(\alpha)$ where $\alpha = \sqrt{2} + \sqrt{3}$. Clearly, $\mathbb{Q}(\alpha) \subseteq L$. Moreover, we have that α has minimal polynomial $g(x) = x^4 - 10x^2 + 1$. Thus, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(g) = 4$. It follows that $L = \mathbb{Q}(\alpha)$.

In order to use Theorem 4.2.9, we must first check that $|S/\mathbb{Z}[\alpha]|$ is not divisible by 3. Expressing $\left\{1, \sqrt{3}, \sqrt{2}, \frac{\sqrt{2}+\sqrt{6}}{2}\right\}$ in terms of the basis $\{1, \alpha, \alpha^2, \alpha^3\}$, we obtain

$$\begin{pmatrix} 1 \\ \sqrt{2} \\ \sqrt{3} \\ \frac{\sqrt{2}+\sqrt{6}}{2} \end{pmatrix} = \begin{pmatrix} 1 \\ -\frac{9}{2}\alpha + \frac{1}{2}\alpha^3 \\ \frac{11}{2}\alpha - \frac{1}{2}\alpha^3 \\ -\frac{5}{4} - \frac{9}{4}\alpha + \frac{1}{4}\alpha^2 + \frac{1}{4}\alpha^3 \end{pmatrix}.$$

Thus,

$$\begin{aligned}
S &= \mathbb{Z} \oplus \mathbb{Z}\sqrt{2} \oplus \mathbb{Z}\sqrt{3} \oplus \mathbb{Z}\left(\frac{\sqrt{2}+\sqrt{6}}{2}\right) \\
&= \mathbb{Z} \oplus \mathbb{Z}\left(\frac{\alpha^3 - 9\alpha}{2}\right) \oplus \mathbb{Z}\left(\frac{11\alpha - \alpha^3}{2}\right) \oplus \mathbb{Z}\left(\frac{\alpha^3 + \alpha^2 - 9\alpha - 5}{4}\right) \\
&= \mathbb{Z} \oplus \mathbb{Z}\left(\frac{\alpha^3 - 9\alpha}{2} + \frac{11\alpha - \alpha^3}{2}\right) \oplus \mathbb{Z}\left(\frac{11\alpha - \alpha^3}{2}\right) \oplus \mathbb{Z}\left(\frac{\alpha^3 + \alpha^2 - 9\alpha - 5}{4}\right) \\
&= \mathbb{Z} \oplus \mathbb{Z}\alpha \oplus \mathbb{Z}\left(\frac{11\alpha - \alpha^3}{2} + 2\left(\frac{\alpha^3 + \alpha^2 - 9\alpha - 5}{4}\right)\right) \oplus \mathbb{Z}\left(\frac{\alpha^3 + \alpha^2 - 9\alpha - 5}{4}\right) \\
&= \mathbb{Z} \oplus \mathbb{Z}\alpha \oplus \mathbb{Z}\left(\frac{\alpha^2 + 2\alpha - 5}{2}\right) \oplus \mathbb{Z}\left(\frac{\alpha^3 + \alpha^2 - 9\alpha - 5}{4}\right)
\end{aligned}$$

Hence, $S \subseteq \frac{1}{4}\mathbb{Z}[\alpha]$. Since

$$2^8 = 4^4 = \left|\frac{1}{4}\mathbb{Z}[\alpha]/\mathbb{Z}[\alpha]\right| = \left|\frac{1}{4}\mathbb{Z}[\alpha]/S\right| \left|S/\mathbb{Z}[\alpha]\right|,$$

we conclude that $|S/\mathbb{Z}[\alpha]|$ divides 2^8, so 3 does not divide $|S/\mathbb{Z}[\alpha]|$.

We have that $g(x) \equiv (x^2+1)^2 \pmod 3$. By Theorem 4.2.9, we obtain that $3S = Q^2$ where

$$Q = (3, \alpha^2 + 1).$$

It immediately follows that $Q = (\sqrt{3})$ and $3S = (\sqrt{3})^2$. Hence, $e(Q \mid 3) = 2$ and the number of primes of S lying over 3 is $r = 1$. Consequently, Theorem 4.2.5 implies that $f(Q \mid 3) = 2$.

4.3 Splitting of Primes in Normal Extensions

Suppose L is a normal extension of K with Galois group $G = \mathrm{Gal}(L/K)$, and let $\sigma \in G$. By Lemma 3.2.3, $\sigma(S) = S$, so $\sigma|_S$ is an automorphism of S. Moreover, since σ fixes K pointwise, we must have that $\sigma(P) = P$. Consequently, $\sigma(PS) = PS$. We must have that σ maps ideals of S to ideals of S, so σ must permute the prime ideals lying over P. A natural question is what are the orbits of the primes lying over P?

Theorem 4.3.1. *Suppose L is a normal extension of K. Let $R = \mathcal{O}_K$, $S = \mathcal{O}_L$, and let Q and Q' be two primes of S lying over the same prime P of R. Then there exists some $\sigma \in G = \mathrm{Gal}(L/K)$ such that $\sigma(Q) = Q'$. That is, G acts transitively on the primes of S lying over P.*

Suppose $\sigma(Q) = Q'$ for $\sigma \in G = \mathrm{Gal}(L/K)$. Since $\sigma(PS) = PS$, we must have that Q and Q' have the same exponent in the prime factorization of PS. Hence, $e(Q \mid P) = e(Q' \mid P)$. Moreover, $S/Q \cong \sigma(S)/\sigma(Q) = S/Q'$, so the residual fields S/Q and S/Q' are isomorphic. Consequently, $f(Q \mid P) = [S/Q \ : \ R/P] = [S/Q' \ : \ R/P] = f(Q' \mid P)$.

Corollary 4.3.2. *If L is a normal extension of K and Q, Q' are two primes lying over P, then $e(Q \mid P) = e(Q' \mid P)$ and $f(Q \mid P) = f(Q' \mid P)$.*

For normal extensions, all primes lying over P have the same ramification index and inertial degree. In this case, Theorem 4.2.5 gives us the following:

Corollary 4.3.3. *Suppose L is a normal extension of K of degree n. Let r be the number of primes of S lying over a prime P of R. Let Q be a prime of S lying over P, $e = e(Q \mid P)$, and $f = f(Q \mid P)$. Then $n = ref$.*

Example 4.3.4. Let $g(x) = x^3 - 3x - 3$, α be a root of g, and let $L = \mathbb{Q}(\alpha)$. We claim that L is a nonnormal extension of $\mathbb{Q}$ of degree 3. Let M be the splitting field of g. We must show that $L \subsetneq M$. Using Maple, we computed that $\Delta(g) = -3^3 \cdot 5$. Since $\sqrt{\Delta(g)} \notin \mathbb{Q}$, Prop. 2.6.2 gives us that $\mathrm{Gal}(M/\mathbb{Q})$ is not isomorphic to a subgroup of A_3. Since $\mathrm{Gal}(M/\mathbb{Q})$ is isomorphic to a subgroup of S_3, we must have that $\mathrm{Gal}(M/\mathbb{Q}) \cong S_3$. Hence, $[M : \mathbb{Q}] = |\mathrm{Gal}(M/\mathbb{Q})| = 6$. But $[L : \mathbb{Q}] = \deg(g) = 3$. Thus, $L \subsetneq M$, so L is a nonnormal extension of $\mathbb{Q}$.

How does (5) split in L? We have that $g(x) \equiv (x-1)^2(x+2) \pmod 5$. We would like to use Theorem 4.2.9 to say that $5S = Q_1^2 Q_2$ where $Q_1 = (5, \alpha - 1)$, $Q_2 = (5, \alpha + 2)$, and $S = \mathcal{O}_L$; however, without knowledge of what S is, we cannot directly determine if $|S/\mathbb{Z}[\alpha]|$ is divisible by 5. Luckily, Props. 3.3.2 and 3.3.7 imply that

$$-3^3 \cdot 5 = \Delta(g) = \Delta(\mathbb{Z}[\alpha]) = |S/\mathbb{Z}[\alpha]|^2 \Delta(S).$$

Thus, $|S/\mathbb{Z}[\alpha]|^2$ divides $-3^3 \cdot 5$, so 5 does not divide $|S/\mathbb{Z}[\alpha]|$. We can now apply Theorem 4.2.9 to obtain $5S = Q_1^2 Q_2$, $e(Q_1 \mid 5) = 2$, $e(Q_2 \mid 5) = 1$, $f(Q_1 \mid 5) = 1$, and $f(Q_2 \mid 5) = 1$. This shows that the ramification indices may be different when L is a nonnormal extension of K.

Example 4.3.5. Let $L = \mathbb{Q}(\sqrt[3]{2})$. As we saw in Example 2.2.4, L is a nonnormal extension of $\mathbb{Q}$ of degree 3. We have that L has ring of integers $S = \mathbb{Z}[\sqrt[3]{2}]$. How does (5) split in L?

We have that $\sqrt[3]{2}$ has minimal polynomial $g(x) = x^3 - 2$. Moreover, $|S/\mathbb{Z}[\sqrt[3]{2}| = 1$ is not divisible by 5 and $\overline{g}(x) \equiv (x-1)(x^2+3x+4) \pmod 5$ is a factorization of $\overline{g}$ into irreducibles in $\mathbb{Z}/5\mathbb{Z}$. Applying Theorem 4.2.9, we obtain that $5S = Q_1Q_2$ is the prime factorization of $5S$ where $Q_1 = (5, \sqrt[3]{2} - 1)$ and $Q_2 = (5, \sqrt[3]{4} + 3\sqrt[3]{2} + 4)$. Moreover, $e_1 = e(Q_1 \mid 5) = 1$, $e_2 = e(Q_2 \mid 5) = 1$, $f(Q_1 \mid 5) = 1$, and $f(Q_2 \mid 5) = 2$. This shows that the inertia degrees may be different when L is a nonnormal extension of K.

Example 4.3.6. Let $L = \mathbb{Q}(\sqrt{3}, \sqrt{7})$. Then $S = \mathcal{O}_L$ is the $\mathbb{Z}$-module generated by $\left\{1, \sqrt{3}, \frac{\sqrt{3}+\sqrt{7}}{2}, \frac{1+\sqrt{21}}{2}\right\}$. How does (3) split in L? We claim that L is normal over $\mathbb{Q}$. Arguing similarly as we did in Example 4.2.10, it is easy to show that $L = \mathbb{Q}(\alpha)$ where $\alpha = \sqrt{3} + \sqrt{7}$. Moreover, α has minimal polynomial $g(x) = x^4 - 20x^2 + 16$. The roots of g are $\pm\sqrt{3} \pm \sqrt{7}$ with all possible combinations of $+$ and $-$. Since all of these roots lie in L and $L = \mathbb{Q}(\alpha)$, it follows that L is the splitting field of g. Thus, L is normal over $\mathbb{Q}$.

Since L is normal over $\mathbb{Q}$, Corollary 4.3.2 implies that all primes Q of S lying over (3) have the same ramification index e and inertial degree f. We consider how 3 splits in the subfields $\mathbb{Q}(\sqrt{3})$ and $\mathbb{Q}(\sqrt{7})$. It is easy to show that

$$3\mathbb{Z}[\sqrt{3}] = (\sqrt{3})^2,$$

and since e is multiplicative, we must have that $e \geq 2$. Similarly,

$$3\mathbb{Z}[\sqrt{7}] = (3, 1 + \sqrt{7})(3, 1 - \sqrt{7}),$$

so $r \geq 2$. Since $n = [L : \mathbb{Q}] = 4$, Corollary 4.3.3 gives us that $4 = n = ref \geq 4f$. Consequently, we must have that $r = 2$, $e = 2$, and $f = 1$. Indeed, proceeding similarly as we did in Example 4.2.10, we would obtain the prime factorization

$$3S = (3, \sqrt{3} + \sqrt{7} + 1)^2(3, \sqrt{3} + \sqrt{7} + 2)^2.$$

4.4 Ramification and the Discriminant

Surprisingly, it turns out the discriminant encodes information about what primes of $\mathbb{Z}$ ramify in a number field L.

Theorem 4.4.1. *Let p be a prime in $\mathbb{Z}$, L be a number field, and $S = \mathcal{O}_L$. Then p ramifies in S if and only if $p \,\big|\, \Delta(S)$.*

Example 4.4.2. Consider the quadratic extension $L = \mathbb{Q}(\sqrt{3})$. We saw in Example 3.1.10 that $S = \mathcal{O}_L = \mathbb{Z}[\sqrt{3}]$, and in Example 3.3.10 we saw that $\Delta(S) = 4 \cdot 3 = 2^2 \cdot 3$. It follows by Theorem 4.4.1 that the only primes of $\mathbb{Z}$ which ramify in L are 2 and 3. In this case, the ramification indices satisfy $e > 1$, and since $n = [L : \mathbb{Q}] = 2$, we must have that 2 and 3 are totally ramified in L.

Example 4.4.3. Consider the cyclotomic field $L = \mathbb{Q}(\omega_{p^k})$ where p is a prime. Then $S = \mathbb{Z}[\omega_{p^k}]$. Which primes of $\mathbb{Z}$ ramify in S? In Example 3.3.12, we saw that

$$\begin{aligned}\Delta(S) &= \pm\frac{\left(p^k\right)^{\varphi(p^k)}}{p^{\varphi(p^k)/(p-1)}} \\ &= \pm p^{p^{k-1}(kp-k-1)}\end{aligned}$$

with the $+$ sign if and only if $\varphi(p^k) \equiv 1 \pmod 4$. Excluding the case when $p = 2$ and $k = 1$ where $L = \mathbb{Q}$, we have that $kp - k - 1 > 0$. Thus, if $p \neq 2$ or $k \neq 1$, then the only prime dividing $\Delta(S)$ is p. By Theorem 4.4.1, in this case p is the only prime that ramifies in L. As we saw in Example 4.2.6, not only does p ramify in L, p is totally ramified in L. However, $\Delta(S)$ gives no indication of how large the ramfication index is; it only tells us that p is ramified.

Example 4.4.4. Let $g(x) = x^3 - 9x + 3$, α be a root of g, and $L = \mathbb{Q}(\alpha)$. Which primes of $\mathbb{Z}$ ramify in $S = \mathcal{O}_L$? In this case, we do not know what the ring S is, so $\Delta(S)$ cannot be actually calculated. However, we can compute $\Delta(\mathbb{Z}[\alpha]) = \Delta_{L/\mathbb{Q}}(\alpha) = \Delta(g)$. Using Maple, we computed $\Delta(g) = 3^5 \cdot 11$. Since both $\mathbb{Z}[\alpha]$ and S are $\mathbb{Z}$-modules of rank $n = [L : \mathbb{Q}] = 3$ with $\mathbb{Z}[\alpha] \subseteq S$, Prop. 3.3.7 gives us that

$$3^5 \cdot 11 = \Delta(\mathbb{Z}[\alpha]) = |S/\mathbb{Z}[\alpha]|^2 \Delta(S).$$

Since 3 and 11 have odd exponents in $\Delta(\mathbb{Z}[\alpha])$, it must be the case that 3 and 11 divide $\Delta(S)$. Moreover, since $\Delta(S) \,\Big|\, \Delta(\mathbb{Z}[\alpha])$, it must be the case that 3 and 11 are the only primes of $\mathbb{Z}$ that divide $\Delta(S)$. Thus, by Theorem 4.4.1 we obtain that 3 and 11 are the only primes of $\mathbb{Z}$ that ramify in L.

4.5 The Different

The discriminant gives us a complete answer to which primes p of $\mathbb{Z}$ ramify in a given number field L. But what if the base field K is not $\mathbb{Q}$? This result does not hold for

arbitrary K. Moreover, the discriminant does not actually tell us which primes Q of S are ramified over p. As it turns out, there is an ideal of S called the different that addresses these shortcomings of the discriminant.

Recall from Ch.3 that the trace $T_{L/K}$ is an additive map from $L \to K$. Given a basis $\{\alpha_1, ..., \alpha_n\}$ for L over K, there exists a dual basis $\{\beta_1, ..., \beta_n\}$ with respect to $T_{L/K}$. For the case when $\{\alpha_1, ..., \alpha_n\}$ is a basis for S as an R-module, we will use the dual basis to define the different.

Proposition 4.5.1. *Let $\{\alpha_1, ..., \alpha_n\}$ be a basis for L over K. Then there exists $\beta_1, ..., \beta_n \in L$ such that*

$$T_{L/K}(\alpha_i \beta_j) = \delta_{ij} = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{otherwise.} \end{cases}$$

Moreover, $\{\beta_1, ..., \beta_n\}$ is another basis for L over K. That is, $\{\beta_1, ..., \beta_n\}$ is the dual basis to $\{\alpha_1, ..., \alpha_n\}$ with respect to $T_{L/K}$.

Let A be an R-module generated by $\{\alpha_1, ..., \alpha_n\}$. Let $\{\beta_1, ..., \beta_n\}$ be the dual basis. We define A^* to be the R-module generated by $\{\beta_1, ..., \beta_n\}$. We define the **different** of A over R to be

$$\text{diff}(A \mid R) = (A^*)^{-1}$$

where

$$A^{-1} = \{\alpha \in L \mid \alpha A \subseteq S\}.$$

Although the definition of the different may be uninspiring and unintuitive at first glance, it turns out that the different tells us which primes Q of S are ramified over $P = Q \cap R$.

Theorem 4.5.2. *Suppose P is a prime of R, Q is a prime of S lying over P, and $e = e(Q \mid P)$. Then $Q^{e-1} \Big| \text{diff}(S \mid R)$. Thus, if Q is ramified over P, then $Q \Big| \text{diff}(S \mid R)$. Conversely, if $Q \Big| \text{diff}(S \mid R)$, then Q is ramified over P.*

The different $\text{diff}(S \mid R)$ is an ideal of S whose prime divisors are precisely the primes Q which ramify over P. It tells us more than just whether P ramifies in S or not; it tells us which prime Q is ramified over P. Moreover, unlike the discriminant, this result is true for any arbitrary base field K.

The different has a couple more important properties that we will need in our proof of the Kronecker-Weber Theorem. We list them here.

Proposition 4.5.3 (diff are multiplicative in towers)**.** *Suppose K, L, and M are number fields with $K \subseteq L \subseteq M$. Let $R = \mathcal{O}_K$, $S = \mathcal{O}_L$, and $T = \mathcal{O}_M$. Then*

$$\mathrm{diff}(T \mid R) = \mathrm{diff}(T \mid S)(\mathrm{diff}(S \mid R)T).$$

Proposition 4.5.4. *Let P be a prime of R and Q be a prime of S lying over P. Let $\pi \in Q \setminus Q^2$ and f be the minimal polynomial for π over K. Suppose that Q is totally ramified over P. Then the exact power of Q in* $\mathrm{diff}(S \mid R)$ *is the same as that in $f'(\pi)S$.*

For more information on the different and for proofs of these results, the reader may refer to [2] and [5].

Chapter 5

Decomposition, Inertia, and Ramification Groups

5.1 Introduction

The goal of this chapter is to show the relationship between subgroups of the Galois group and the splitting of primes in the corresponding fixed field. For this chapter, we will assume that L and K are number fields with L being a normal extension of K of degree n. We will let $R = \mathcal{O}_K$, $S = \mathcal{O}_L$, and $G = \text{Gal}(L/K)$. Let P be a prime of R and Q be a prime of S lying over P. As before, we will let $e = e(Q \mid P)$, $f = f(Q \mid P)$, and r denote the number of primes of S lying over P. We define two important subgroups of the Galois group G: the **decomposition group**

$$D = D(Q \mid P) = \{\sigma \in G \mid \sigma(Q) = Q\}$$

and the **inertia group**

$$E = E(Q \mid P) = \{\sigma \in G \mid \sigma(\alpha) \equiv \alpha \pmod{Q} \text{ for all } \alpha \in S\}.$$

The fixed field L^D is called the **decomposition field** and the fixed field L^E is the **inertia field**. We have that $E \leq D$ since for all $\sigma \in E$, if $\alpha \in Q$, then $\sigma(\alpha) \equiv \alpha \equiv 0 \pmod{Q}$, so $\sigma(Q) = Q$.

Example 5.1.1. As we did in Example 4.2.10, consider the number field $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Then L is a normal extension of $\mathbb{Q}$ with $G = \text{Gal}(L/\mathbb{Q}) = \{\text{id}, \sigma_1, \sigma_2, \sigma_3\}$ where

$$\sigma_1 : \begin{cases} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt{3} \mapsto -\sqrt{3} \end{cases} \qquad \sigma_2 : \begin{cases} \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt{3} \mapsto \sqrt{3} \end{cases} \qquad \sigma_3 : \begin{cases} \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt{3} \mapsto -\sqrt{3} \end{cases}$$

We have that $S = \mathcal{O}_L$ is the $\mathbb{Z}$-module generated by $\left\{1, \sqrt{3}, \sqrt{2}, \frac{\sqrt{2}+\sqrt{6}}{2}\right\}$. We also showed in Example 4.2.10 that the prime factorization of $3S$ is $3S = Q^2$ where $Q = (\sqrt{3}) = (\sqrt{6})$. What is the decomposition group $D = D(Q \mid 3)$, the inertia group $E = E(Q \mid 3)$, the decomposition field L^D, and the inertia field L^E? It is easy to see that Q is fixed by all automorphisms in G. Hence, $D = G$ and the corresponding fixed field is $L^D = L^G = \mathbb{Q}$. If

$\alpha = a + b\sqrt{3} + c\sqrt{2} + d\frac{\sqrt{2}+\sqrt{6}}{2}$ is an element of S, then

$$\begin{aligned}\sigma_1(\alpha) &= a - b\sqrt{3} + c\sqrt{2} + d\frac{\sqrt{2}-\sqrt{6}}{2} \\ &= a + b\sqrt{3} + c\sqrt{2} + d\frac{\sqrt{2}+\sqrt{6}}{2} - 2b\sqrt{3} - d\sqrt{6} \\ &= \alpha - 2b\sqrt{3} - d\sqrt{6} \\ &\equiv \alpha \pmod{Q}.\end{aligned}$$

Hence, $\sigma_1 \in E$. On the other hand, $\sigma_2(\sqrt{2}) = -\sqrt{2} \not\equiv \sqrt{2} \pmod{Q}$ since this would imply $2\sqrt{2} \in Q$ which in turn would imply $1 = 3^2 - (2\sqrt{2})^2 \in Q$, so $Q = S$. Thus, $\sigma_2 \notin E$. Since E is a subgroup of G, it follows that $E =< \sigma_1 >$. The corresponding fixed field is $L^E = \mathbb{Q}(\sqrt{2})$.

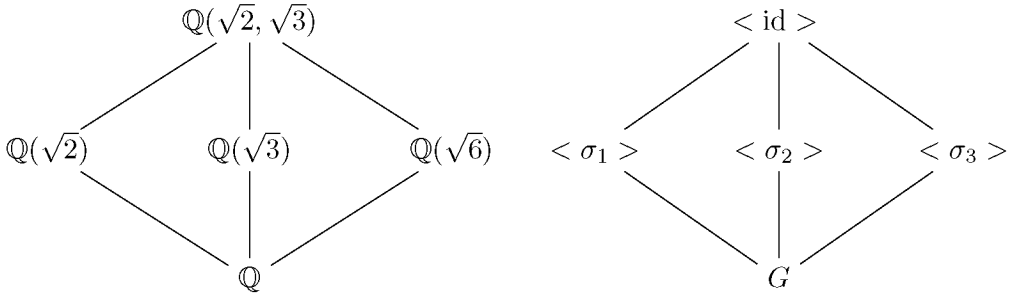


Figure 5.1. The Galois correspondence for $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$

As it turns out, the quotient D/E is isomorphic to $\overline{G} = \mathrm{Gal}(S/Q \ / \ R/P)$. We will show for now only that D/E can be embedded into $\overline{G}$.

Lemma 5.1.2. *With the notation as above, E is a normal subgroup of D and there is an embedding $D/E \hookrightarrow \overline{G} = \mathrm{Gal}(S/Q \ / \ R/P)$.*

Proof. For $\sigma \in G$, we have that σ restricts to an automorphism of S (by Lemma 3.2.3). If $\alpha_1 \equiv \alpha_2 \pmod{Q}$ for $\alpha_1, \alpha_2 \in S$, then $\alpha_1 - \alpha_2 \in Q$. Hence, for all $\sigma \in D$, we have that $\sigma(\alpha_1) - \sigma(\alpha_2) = \sigma(\alpha_1 - \alpha_2) \in \sigma(Q) = Q$. That is, $\sigma(\alpha_1) \equiv \sigma(\alpha_2) \pmod{Q}$. Hence, $\sigma \in D$ induces a well-defined automorphism $\overline{\sigma} : S/Q \to S/Q$. Let $\psi : S \to S/Q$ denote the projection map. Then

$$\psi \circ \sigma : \alpha \mapsto \sigma(\alpha) \mapsto \sigma(\alpha) \pmod{Q},$$

and

$$\overline{\sigma} \circ \psi : \alpha \mapsto \alpha \pmod{Q} \mapsto \sigma(\alpha) \pmod{Q}.$$

All this is to say that the following diagram commutes:

$$\begin{array}{ccc} S & \xrightarrow{\sigma} & S \\ {\scriptstyle\psi}\downarrow & & \downarrow{\scriptstyle\psi} \\ S/Q & \xrightarrow{\overline{\sigma}} & S/Q \end{array}$$

Since σ fixes K (and hence R) pointwise, it follows that $\overline{\sigma}$ fixes $R/(Q \cap R) = R/P$ pointwise. Thus, $\overline{\sigma}$ is a member of the Galois group $\overline{G}$ of S/Q over R/P. The map $\sigma \mapsto \overline{\sigma}$ gives us a homomorphism $D \to \overline{G}$. The kernel of this homomorphism is the set of $\sigma \in D$ with $\sigma(\alpha) \equiv \alpha \pmod{Q}$; that is, the kernel is E. In particular, this implies E is a normal subgroup of D. By the First Isomorphism Theorem, we have an embedding $D/E \hookrightarrow \overline{G}$. $\square$

5.2 The Main Result

Given a subgroup $H \leq G$, it is easy to see that for any set $X \subseteq L$ that the subset of X fixed by H is $X^H = X \cap L^H$. This gives us that the set $S^H = \mathcal{O}_{L^H}$. In the ring S^H, we have that $Q^H = Q \cap L^H$ must be a prime ideal lying under Q (by Prop. 4.1.1). Moreover, $P = Q \cap K = Q^H \cap K$, so Q^H lies over P (again by Prop. 4.1.1). All of this is to say S^H is the ring of algebraic integers in L^H, and Q^H is a prime ideal of S^H lying over P and lying under Q.

With this in mind, we turn now to the most important result of this chapter. It gives a relationship between certain subgroups of the Galois group $\mathrm{Gal}(L/K)$, their corresponding fixed fields, and how primes of R split in S.

Theorem 5.2.1. *With the notation as before, we have the following:*

degrees	L	Q	*ramification indices*	*inertial degrees*
e	|	|	e	*1*
	L^E	Q^E		
f	|	|	*1*	f
	L^D	Q^D		
r	|	|	*1*	*1*
	K	P		

Proof. First, we will show that $[L^D : K] = r$. From the Galois correspondence theorem, we have that $[L^D : K]$ is the index of D in G. For a given left coset σD, every map $\sigma\delta$ in the coset (where $\delta \in D$) sends Q to $\sigma\delta(Q) = \sigma(Q)$. Conversely, if $\sigma Q = \tau Q$ for $\sigma, \tau \in G$, then $\tau^{-1}\sigma$ maps Q to itself, so $\tau^{-1}\sigma \in D$. Thus, σ and τ belong to the same left coset of D. Moreover, from Theorem 4.3.1, every prime of S lying over P has the form $\sigma(Q)$ for some $\sigma \in G$. This shows that the map $\sigma(Q) \mapsto \sigma D$ is a one-to-one correspondence between the primes of S lying over P and the left cosets of D. Since there are r primes of S lying over P, there must be r left cosets of D. Therefore, the index of D in G is r, so $[L^D : K] = r$.

Next, we will show that $e(Q^D \mid P) = f(Q^D \mid P) = 1$. We have that L is a normal extension of L^D, so by Theorem 4.3.1 the Galois group $\mathrm{Gal}(L/L^D)$ acts transitively on the primes of L lying over Q^D. However, $\mathrm{Gal}(L/L^D) = D$ and D fixes Q, so Q must be the only prime of S lying over Q^D. By Corollary 4.3.3, we have that $[L : L^D] = e(Q \mid Q^D)f(Q \mid Q^D)$. However,

$$[L : L^D]r = [L : L^D][L^D : K] = [L : K] = ref.$$

Hence, $e(Q \mid Q^D)f(Q \mid Q^D) = [L : L^D] = ef$. But $e(Q \mid Q^D) \leq e(Q \mid P) = e$ and $f(Q \mid Q^D) \leq f(Q \mid P) = f$, so the only possibility is that $e(Q \mid Q^D) = e$ and $f(Q \mid Q^D) = f$. Using the fact that e and f are multiplicative in towers, we obtain that $e(Q^D \mid P) = f(Q^D \mid P) = 1$.

Next, we will show that $f(Q \mid Q^E) = 1$. It will suffice to show that the Galois group of S/Q over S^E/Q^E is trivial. We will show that for each $\theta \in S/Q$ that the polynomial $(x - \theta)^{|E|}$ has coefficients in S^E/Q^E. It follows that every member of the Galois group sends θ to another root of $(x - \theta)^{|E|}$, which must be θ. Hence, every member of the Galois group of S/Q over S^E/Q^E fixes all $\theta \in S/Q$, so the only element of $\mathrm{Gal}(S/Q \ / \ S^E/Q^E)$ is

the identity. The result then follows. Fix $\alpha \in S$ corresponding to $\theta \in S/Q$. Consider the polynomial

$$g(x) = \prod_{\sigma \in E} (x - \sigma(\alpha)).$$

Then g is fixed by E and since all $\sigma(\alpha) \in S$ (by Lemma 3.2.3), the coefficients of g must lie in S^E. Now consider the polynomial $\overline{g} \in (S/Q)[x]$ obtained from reducing mod Q the coefficients of g. Letting bars denote reduction mod Q, we have that each $\overline{\sigma(\alpha)}$ for $\sigma \in E$ must be a root of $\overline{g}$. Since $\sigma \in E$, we have that $\alpha \equiv \sigma(\alpha) \pmod{Q}$. Therefore, all $\overline{\sigma(\alpha)} = \overline{\alpha} = \theta$ for $\sigma \in E$. It follows that $\overline{g}(x) = \prod_{\sigma \in E}(x - \theta) = (x - \theta)^{|E|}$. But g has coefficients in S^E, so $\overline{g}$ must have coefficients in $S^E/(Q \cap S^E) = S^E/Q^E$. Thus, $(x - \theta)^{|E|}$ has coefficients in S^E/Q^E, and the result that $f(Q \mid Q^E) = 1$ follows.

We have already shown that $f(Q \mid Q^E) = 1$ and $f(Q^D \mid P) = 1$. Then

$$f = f(Q \mid P) = f(Q \mid Q^E) f(Q^E \mid Q^D) f(Q^D \mid P) = f(Q^E \mid Q^D).$$

It follows by Corollary 4.3.3 that $[L^E : L^D] \geq f(Q^E \mid Q^D) = f$. But Lemma 5.1.2 gives us an embedding $D/E \hookrightarrow \mathrm{Gal}(S/Q \ / \ R/P)$, which implies that

$$f = |\operatorname{Gal}(S/Q \ / \ R/P)| \geq |D/E| = [L^E : L^D].$$

Hence, it must be that $[L^E : L^D] = f$.

Again using Corollary 4.3.3,

$$e(Q^E \mid Q^D) f = e(Q^E \mid Q^D) f(Q^E \mid Q^D) \leq [L^E : L^D] = f.$$

The only possibility is that $e(Q^E \mid Q^D) = 1$. Finally, we have that

$$e(Q \mid Q^E) = e(Q \mid Q^E) e(Q^E \mid Q^D) e(Q^D \mid P) = e(Q \mid P) = e.$$

□

Corollary 5.2.2. *The embedding $D/E \hookrightarrow \overline{G} = \mathrm{Gal}(S/Q \ / \ R/P)$ from Lemma 5.1.2 is an isomorphism.*

Proof. We have that $|D/E| = [L^E : L^D] = f = |\operatorname{Gal}(S/Q \ / \ R/P)|$. It follows that the embedding is surjective. □

Of significance to us is the following corollary:

Corollary 5.2.3. *If D is a normal subgroup of G, then P splits into r distinct primes $Q_1, ..., Q_r$ in L^D. If E is also normal in G, then each Q_i is inert in L^E. Finally each extension of Q_i becomes an e-th power in L.*

Proof. If D is normal in G, then by the Galois correspondence theorem L^D is a normal extension of K. We know by Theorem 5.2.1 that Q^D has ramification index and inertial degree 1 over P. By Corollary 4.3.2, every prime of S^D lying over P has ramification index and inertial degree 1. Since $[L^D : K] = r$, it follows by Corollary 4.3.3 that there are precisely r primes in S^D lying over P. Since there are also precisely r primes in S lying over P, there must be precisely r primes in S^E lying over P. This means that every prime in S^D lies under a unique prime of S^E. If E is also normal in G, then L^E is a normal extension of K. Since Q^E has ramification index 1 over P, the same must be true for all r primes of S^E (by Corollary 4.3.2). Hence, all primes in S^D are inert in S^E. Lastly, there are r primes of S lying over P and there are r primes of S^E lying over P. It follows that every prime of S^E must lie under a unique prime of S. Since L is a normal extension of K, each of these primes of S has ramification index e over P. Since each prime of S^E has ramification index 1 over P, it follows from the multiplicity in towers of ramification indices (Prop. 4.2.2) that every prime in S has ramification index e over the corresponding prime in S^E. Thus, each prime of S^E lying over P becomes an e-th power in L. □

Corollary 5.2.3 is of tremendous importance to us. We will particularly be interested in normal extensions of $\mathbb{Q}$ with abelian Galois group. In this case, Corollary 5.2.3 always applies. Corollary 5.2.3 also explains the reason for calling L^D the decomposition field: the prime P decomposes into r primes in this field. Similarly, L^E is called the inertia field because the primes of L^D are inert in L^E.

Example 5.2.4. As in Example 5.1.1, again consider the number field $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. We have that $G = \mathrm{Gal}(L/\mathbb{Q}) = \{1, \sigma_1, \sigma_2, \sigma_3\}$ where $\sigma_1, \sigma_2, \sigma_3$ are the same automorphisms as in Example 5.1.1. In particular, $G \cong C_2 \times C_2$ where C_2 is the cyclic group of order 2, so G is abelian. Letting $S = \mathcal{O}_L$, we have the prime factorization $3S = Q^2$ where $Q = (\sqrt{3}) = (\sqrt{6})$. This gives us that $r = 1$ and $e = e(Q \mid 3) = 2$. Since $n = [L : \mathbb{Q}] = 4$, we

deduce from Theorem 4.2.5 that $f = f(Q \mid 3) = 2$. We again ask what is the decomposition group $D = D(Q \mid 3)$, the inertia group $E = E(Q \mid 3)$, the decomposition field L^D, and the inertia field L^E? By Theorem 5.2.1, $[L^D : \mathbb{Q}] = r = 1$, so $L^D = \mathbb{Q}$. Consequently, D is the full Galois group G. Theorem 5.2.1 also gives us that $[L : L^E] = e = 2$, but there are three intermediate fields K with $[L : K] = 2$; namely, $K = \mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{6})$. However, Corollary 5.2.3 implies that that (3) is inert in L^E. In $\mathbb{Q}(\sqrt{2})$, (3) is inert, while in $\mathbb{Q}(\sqrt{3})$ we have $(3) = (\sqrt{3})^2$ and in $\mathbb{Q}(\sqrt{6})$ we have $(3) = (3, \sqrt{6})^2$. Hence, we must have that $L^E = \mathbb{Q}(\sqrt{2})$. Now $\mathbb{Q}(\sqrt{2})$ is the fixed field of $< \sigma_1 >$, so again we obtain $E =< \sigma_1 >$.

Moreover, we have that $D/E \cong C_2$. Since $f = 2$, we know that S/Q has degree 2 over $\mathbb{Z}/3\mathbb{Z}$. This implies that $\overline{G} = \mathrm{Gal}(S/Q \ / \ \mathbb{Z}/3\mathbb{Z}) \cong C_2$. Hence, $D/E \cong \overline{G}$, as predicted by Corollary 5.2.2.

5.3 Some Consequences of the Main Result

Our next result gives some other characterizations of L^D and L^E.

Proposition 5.3.1. *Fix number fields $K \subseteq L$ with L a normal extension of K, and let Q be a prime of $\mathcal{O}_L$. Let K' denote an intermediate field of K and L, and $P' = Q \cap \mathcal{O}_{K'}$. Then*

(1) L^D is the largest K' such that $e(P' \mid P) = f(P' \mid P) = 1$;

(2) L^D is the smallest K' such that Q is the only prime of S lying over P';

(3) L^E is the largest K' such that $e(P' \mid P) = 1$;

(4) L^E is the smallest K' such that Q is totally ramified over P'.

Proof. We will first show that L^D and L^E satisy these properties. The fact that $e(Q^D \mid P) = f(Q^D \mid P) = 1$, $e(Q^E \mid P) = 1$, and that Q is totally ramified over Q^E follows immediately from Theorem 5.2.1. The fact that Q is the only prime of S lying over Q^D was shown in the proof of Theorem 5.2.1.

Let K' be an intermediate field. Then L is normal over K'. Moreover, $K' = L^H$ for some subgroup $H \leq G = \mathrm{Gal}(L/K)$. Then $P' = Q \cap \mathcal{O}_{K'} = Q^H$. For the decomposition

and inertia groups $D' = D(Q \mid Q^H)$ and $E' = E(Q \mid Q^H)$, we have that

$$\begin{aligned} D(Q \mid Q^H) &= \{\sigma \in \mathrm{Gal}(L \,/\, L^H) \mid \sigma(Q) = Q\} \\ &= \{\sigma \in H \mid \sigma(Q) = Q\} \\ &= D \cap H. \end{aligned}$$

Similarly, $E(Q \mid Q^H) = E \cap H$. Hence, by the Galois correspondence theorem $L^{D'} = L^{D \cap H} = L^D L^H = L^D K'$, and similarly $L^{E'} = L^E K'$. Let r' be the number of primes of S lying over Q^H, $e' = e(Q \mid Q^H)$, and $f' = f(Q \mid Q^H)$. Then Theorem 5.2.1 gives us the diagram in Figure 5.2.

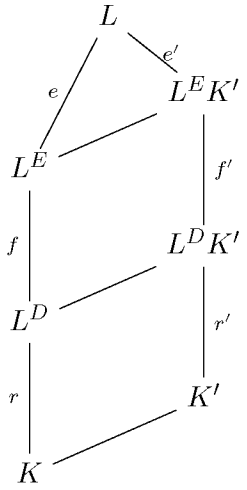


Figure 5.2. The tower of fields in the proof of Prop. 5.3.1.

Using the diagram in Figure 5.2, we will now prove (1) - (4).

(1) Suppose $e(P' \mid P) = f(P' \mid P) = 1$. Then

$$e = e(Q \mid P) = e(Q \mid P')e(P' \mid P) = e(Q \mid P') = e',$$

and similarly $f = f'$. Considering the diagram, we have that $[L : L^D] = [L : L^D K']$. Since $L^D \subseteq L^D K'$, it follows that $L^D = L^D K'$. This implies $K' \subseteq L^D$.

(2) Suppose Q is the only prime of S lying over P'. Then $r' = 1$, which the diagram shows implies $L^D K' = K'$. Hence, $L^D \subseteq K'$.

(3) Suppose $e(P' \mid P) = 1$. As in (1), we have then that $e = e'$. Considering the diagram, we have that $[L : L^E] = [L : L^E K']$ and since $L^E \subseteq L^E K'$, we have then that $L^E = L^E K'$. This shows that $K' \subseteq L^E$.

(4) Suppose Q is totally ramified over P'. Then $[L : K'] = e'$. Hence, $[L : K'] = [L : L^E K']$ and since $K' \subseteq L^E K'$, we obtain $K' = L^E K'$. Thus, $L^E \subseteq K'$.

□

Another consequence of Theorem 5.2.1 is the following result. Suppose P is a prime of K, and L and M are two extensions of K. If P ramifies in L or M, then P must necessarily ramify in LM. This next result shows that the converse is also true: If P is unramified in both L and M, then P is unramified in LM. Thus, we may determine whether or not P ramifies in LM by considering if it ramifies in the smaller fields L and M.

Proposition 5.3.2. *Let K be a number field and let L and M be two extensions of K. Fix a prime P of K. If P is unramified in both L and M, then P is unramified in the composite field LM.*

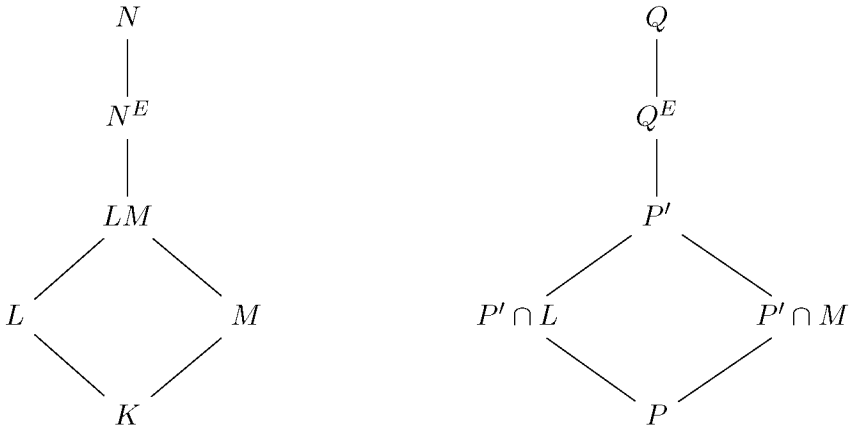


Figure 5.3. Left: The tower of fields in the proof of Prop. 5.3.2; Right: The corresponding tower of primes lying over P.

Proof. Let P' be any prime of LM lying over P. Let N be a normal extension of K containing LM and let Q be a prime of N lying over P'. Then Q also lies over P. Let

$E = E(Q \mid P)$. By Theorem 5.3.1, N^E is the largest intermediate field K' such that $Q \cap K'$ is unramified over P. Consequently, $L \subseteq N^E$ and $M \subseteq N^E$. But then $LM \subseteq N^E$. Since Q^E is unramified over P, $Q^E \cap LM = P'$ must be unramified over P. Thus, P is unramified in LM. □

5.4 Splitting of Primes in Cyclotomic Fields

Theorem 5.4.1 (Splitting of primes in cyclotomic fields). *Suppose $m = p^k n$ where p is a prime of $\mathbb{Z}$ that does not divide n. Let Q be a prime of the m-th cyclotomic field $\mathbb{Q}(\omega_m)$ lying over p. Then*

(1) $e(Q \mid p) = \varphi(p^k)$.

(2) $f(Q \mid p)$ is the order of p in $(\mathbb{Z}/n\mathbb{Z})^*$.

(3) The inertia field $\mathbb{Q}(\omega_m)^{E(Q \mid p)}$ is the n-th cyclotomic field $\mathbb{Q}(\omega_n)$.

Proof. As we saw in Example 4.2.6, $(p) = (1 - \omega_{p^k})^{\varphi(p^k)}$, so p is totally ramified in $\mathbb{Q}(\omega_{p^k})$. That is,

$$e(Q \cap \mathbb{Q}(\omega_{p^k}) \mid p) = [\mathbb{Q}(\omega_{p^k}) : \mathbb{Q}] = \varphi(p^k).$$

Next, we will consider how p splits in $\mathbb{Q}(\omega_n)$. If $n = 1$ or 2, then $\mathbb{Q}(\omega_m) = \mathbb{Q}(\omega_{p^k})$ so p is totally ramified in $\mathbb{Q}(\omega_m)$. In this case, $f(Q \mid p) = 1$, so $f(Q \mid p)$ is trivially the order of p in $(\mathbb{Z}/n\mathbb{Z})^*$. Moreover, we have that $E(Q \mid p) = \mathrm{Gal}(\mathbb{Q}(\omega_m)/\mathbb{Q})$, so the inertia field is $\mathbb{Q} = \mathbb{Q}(\omega_n)$.

Thus, we may suppose $n > 2$. In Example 3.3.12, we saw that for $n > 2$ that

$$\Delta\left(\mathbb{Z}[\omega_n]\right) = (-1)^{\varphi(n)/2} \frac{n^{\varphi(n)}}{\prod_{\substack{q \text{ prime}, \\ q \mid n}} q^{\varphi(n)/(q-1)}}.$$

In particular, $\Delta(\mathbb{Z}[\omega_n]) \,\Big|\, n^{\varphi(n)}$. Since p does not divide n, it follows that p does not divide $\Delta(\mathbb{Z}[\omega_n])$. By Theorem 4.4.1, p is unramified in $\mathbb{Q}(\omega_n)$. By Prop. 5.3.1, the inertia field $\mathbb{Q}(\omega_m)^{E(Q \mid p)}$ is the largest field in which p remains unramified. Thus,
$\mathbb{Q}(\omega_n) \subseteq \mathbb{Q}(\omega_m)^{E(Q \mid p)}$. This implies that

$$e(Q \mid p) = [\mathbb{Q}(\omega_m) : \mathbb{Q}(\omega_m)^{E(Q \mid p)}] \leq [\mathbb{Q}(\omega_m) : \mathbb{Q}(\omega_n)] = \varphi(p^k).$$

Since $e(Q \cap \mathbb{Q}(\omega_{p^k}) \mid p) = \varphi(p^k)$, from the multiplicity of e, we must have that $e(Q \mid p) \geq \varphi(p^k)$. Thus, $e(Q \mid p) = \varphi(p^k)$. Since $\mathbb{Q}(\omega_n) \subseteq \mathbb{Q}(\omega_m)^{E(Q \mid p)}$ and both fields have the same degree over $\mathbb{Q}$, it follows that $\mathbb{Q}(\omega_m)^{E(Q \mid p)} = \mathbb{Q}(\omega_n)$.

Lastly, we must show that $f(Q \mid p)$ is the order of p in $(\mathbb{Z}/n\mathbb{Z})^*$. We have that $f(Q \mid p)$ is the order of $\overline{G} = \mathrm{Gal}(\mathbb{Z}[\omega_m]/Q \ / \ \mathbb{Z}/p\mathbb{Z})$. But $\overline{G}$ is generated by the automorphism $\overline{\phi}$ which maps $\overline{\phi}(x) = x^p$. Hence, $f(Q \mid p)$ is the order of $\overline{\phi}$. Considering the isomorphism $D(Q \mid p)/E(Q \mid p) \cong \overline{G}$ given in Corollary 5.2.2, there is an automorphism $\phi \in D(Q \mid p)$ that corresponds with $\overline{\phi}$, namely a Frobenius automorphism satisfying $\phi(\omega_m) \equiv \omega_m^p \pmod{Q}$. Then $f(Q \mid p)$ is the order of ϕ mod $E(Q \mid p)$. That is, $f(Q \mid p)$ is the minimum integer l such that $\phi^l \in E(Q \mid p)$. Since $\mathbb{Q}(\omega_n) = \mathbb{Q}(\omega_m)^{E(Q \mid p)}$, it follows that $f(Q \mid p)$ is the minimum integer l such that $\phi^l \in \mathrm{Gal}(\mathbb{Q}(\omega_m)/\mathbb{Q}(\omega_n))$. Equivalently, $f(Q \mid p)$ is the minimum integer l such that $\phi^l(\omega_n) = \omega_n$. Hence, $f(Q \mid p)$ is the minimum integer l such that $\omega_n = \phi^l(\omega_n) \equiv \omega_n^{p^l} \pmod{Q \cap \mathbb{Q}(\omega_n)}$. Letting $P = Q \cap \mathbb{Q}(\omega_n)$, we have that $f(Q \mid p)$ is the minimum integer l such that $\omega_n - \omega_n^{p^l} = \omega_n(1 - \omega_n^{p^l - 1}) \in P$.

We claim that

$$(1 - \omega_n)(1 - \omega_n^2)...(1 - \omega_n^{n-1}) = n. \tag{5.1}$$

Assuming this for now, if $p^l \not\equiv 1 \pmod{n}$, then the factor $(1 - \omega_n^{p^l - 1})$ occurs in equation (5.1). It follows that if $p^l \not\equiv 1 \pmod{n}$ and $\omega_n(1 - \omega_n^{p^l - 1}) \in P$, then by multiplying by the missing factors in equation (5.1), we obtain $n\omega_n \in P$. Since ω_n is a unit in $\mathbb{Z}[\omega_n]$, we would have that $n \in P$, and hence $n \in P \cap \mathbb{Z} = p\mathbb{Z}$. However, p does not divide n, so we must have that $p^l \equiv 1 \pmod{n}$ if and only if $\omega_n(1 - \omega_n^{p^l - 1}) \in P$. Therefore, $f(Q \mid p)$ is the minimum integer l such that $p^l \equiv 1 \pmod{n}$. Hence, $f(Q \mid p)$ is the order of p in $(\mathbb{Z}/n\mathbb{Z})^*$. Thus, if equation (5.1) is true, then $f(Q \mid p)$ is the order of p in $(\mathbb{Z}/n\mathbb{Z})^*$

We now establish equation (5.1). Let $f(x) = \frac{x^n - 1}{x - 1} = x^{n-1} + x^{n-2} + ... + x + 1$. We have that the roots of f are the n-th roots of unity not equal to 1. Thus,

$$f(x) = (x - \omega_n)(x - \omega_n^2)...(x - \omega_n^{n-1}).$$

Therefore, $f(1) = (1 - \omega_n)(1 - \omega_n^2)...(1 - \omega_n^{n-1})$. However, $f(x) = x^{n-1} + x^{n-2} + ... + x + 1$, so $f(1) = n$. Hence,

$$(1 - \omega_n)(1 - \omega_n^2)...(1 - \omega_n^{n-1}) = n.$$

□

Example 5.4.2. Consider the 21-st cyclotomic field $L = \mathbb{Q}(\omega_{21})$. Then $n = [L : \mathbb{Q}] = \varphi(21) = 12$ and $G = \mathrm{Gal}(L/\mathbb{Q}) \cong (\mathbb{Z}/21\mathbb{Z})^*$. Let Q be a prime of S lying over $p = 3$. Then $e = e(Q \mid 3) = \varphi(3) = 2$, and $f = f(Q \mid 3)$ is the order of 3 in $(\mathbb{Z}/7\mathbb{Z})^*$, which is 6. Then $12 = n = ref = 12r$, so $r = 1$. By Theorem 5.4.1, $|D| = [L : L^D] = ef = 12$, so $D = G$. Similarly, $|E| = [L : L^E] = e = 2$, so E must be a subgroup of G of order 2. There is only one such subgroup, namely the one corresponding to $< 8 >$ under the isomorphism $G \cong (\mathbb{Z}/21\mathbb{Z})^*$. Hence, $E =< \sigma >$ where $\sigma : \omega_{21} \mapsto \omega_{21}^8$.

5.5 Ramification Groups

Related to the decomposition and inertia groups are ramification groups. As it turns out, these ramification groups are related to the different via Hilbert's Formula. As we saw in Chapter 4, the different tells us which primes Q of S are ramified over $P = Q \cap R$. This gives us another connection between subgroups of the Galois group and ramification of primes. We will need this connection in our proof of the Kronecker-Weber Theorem in Chapter 6.

With the same notation as above, for all $m \geq 0$ we define the **m-th ramification group**

$$V_m = V_m(Q \mid P) = \{\sigma \in G \mid \sigma(\alpha) \equiv \alpha \pmod{Q^{m+1}} \text{ for all } \alpha \in S\}$$

Thus, $E = V_0 \geq V_1 \geq V_2 \geq ...$ form a descending chain of subgroups. It is easily verified from the definition that all V_m are normal subgroups of D.

The quotient group V_{m-1}/V_m can be related to some groups that are easier to understand. In particular, we will show that $V_0/V_1 \hookrightarrow (S/Q)^*$ and $V_{m-1}/V_m \hookrightarrow S/Q$ for $m \geq 2$. Since S/Q is a finite field, as an additive group S/Q is isomorphic to $f(Q \mid p)$ direct summands of $\mathbb{Z}/p\mathbb{Z}$ where $p = Q \cap \mathbb{Z}$. Moreover, $(S/Q)^*$ is a cyclic group of order $\|Q\| - 1$. Viewing V_{m-1}/V_m as a subgroup of $(S/Q)^*$ or S/Q will allow us to understand the structure of these ramification groups. Before we prove that these embeddings exist, we will need a few lemmas.

Lemma 5.5.1. *With the notation as above, $S = S^E + Q$.*

Proof. We have that $f(Q \mid Q^E) = 1$ by Theorem 5.2.1, so $S^E/Q^E \cong S/Q$. Now $S^E + Q$ is a subring of S with ideal Q, so $(S^E + Q)/Q \subseteq S/Q$. We claim that S/Q is isomorphic to $(S^E + Q)/Q$. Let $\psi : S^E \to (S^E + Q)/Q$ map $\psi(s) = s + Q$. Then ψ is clearly a

homomorphism. Moreover,

$$\ker \psi = S^E \cap Q = Q^E.$$

By the First Isomorphism Theorem, $S^E/Q^E \hookrightarrow (S^E + Q)/Q$. This implies

$$|S/Q| = |S^E/Q^E| \leq |(S^E + Q)/Q| \leq |S/Q|,$$

so $|(S^E + Q)/Q| = |S/Q|$. Hence, $(S^E + Q)/Q = S/Q$ which gives us that $S^E + Q = S$. $\square$

Proposition 5.5.2. *Fix an element $\pi \in Q \setminus Q^2$. Then for any $\sigma \in V_{m-1}$ $(m \geq 1)$ we have that $\sigma \in V_m$ if and only if $\sigma(\pi) \equiv \pi \pmod{Q^{m+1}}$.*

Proof. If $\sigma \in V_m$, then $\sigma(\pi) \equiv \pi \pmod{Q^{m+1}}$ by definition. Conversely, suppose $\sigma(\pi) \equiv \pi \pmod{Q^{m+1}}$. We must show that $\sigma(\alpha) \equiv \alpha \pmod{Q^{m+1}}$ for all $\alpha \in S$. First we will prove the result for all $\alpha \in \pi S$. Let $\alpha \in \pi S$. Then $\alpha = \pi s$ for some $s \in S$. We have that

$$\begin{aligned}
\sigma(\alpha) - \alpha &= \sigma(\pi)\sigma(s) - \pi s \\
&= \sigma(\pi)\sigma(s) - \pi\sigma(s) + \pi\sigma(s) - \pi s \\
&= \sigma(s)(\sigma(\pi) - \pi) + \pi(\sigma(s) - s).
\end{aligned}$$

Since $\sigma(\pi) \equiv \pi \pmod{Q^{m+1}}$, $\sigma(\pi) - \pi \in Q^{m+1}$. Since $\sigma \in V_{m-1}$, $\sigma(s) \equiv s \pmod{Q^m}$, so $\pi(\sigma(s) - s) \in Q^{m+1}$. It follows that $\sigma(\alpha) - \alpha \in Q^{m+1}$, so $\sigma(\alpha) \equiv \alpha \pmod{Q^{m+1}}$.

Next, we will prove the result for all $\alpha \in Q$. Since $\pi \in Q \setminus Q^2$, we have that $\pi S = QI$ for some ideal I not divisible by Q. Pick $\beta \in I \setminus Q$. Then $\beta \notin Q$ but for any $\alpha \in Q$, we have $\alpha\beta \in QI = \pi S$. Then

$$\begin{aligned}
(\sigma(\beta) - \beta)\sigma(\alpha) + \beta\sigma(\alpha) &= \sigma(\beta)\sigma(\alpha) \\
&= \sigma(\beta\alpha) \\
&\equiv \beta\alpha \pmod{Q^{m+1}}.
\end{aligned}$$

where the last equality follows from the previous argument. But $\sigma(\beta) - \beta \in Q^m$ since $\sigma \in V_{m-1}$ and $\sigma(\alpha) \equiv \alpha \equiv 0 \pmod{Q}$, so
$(\sigma(\beta) - \beta)\sigma(\alpha) \equiv 0 \pmod{Q^{m+1}}$. Hence, $\beta\sigma(\alpha) \equiv \beta\alpha \pmod{Q^{m+1}}$. But $\beta \notin Q$, so it must be the case that $\sigma(\alpha) \equiv \alpha \pmod{Q^{m+1}}$.

Finally, we will prove the result for all $\alpha \in S$. From Lemma 5.5.1, we have that $S = S^E + Q$. Then for any $\alpha \in S$, we have $\alpha = \beta + \gamma$ for some $\beta \in S^E$ and $\gamma \in Q$. We have that $\sigma \in E$, so $\sigma(\beta) = \beta$. By the previous argument, $\sigma(\gamma) \equiv \gamma \pmod{Q^{m+1}}$, so

$$\sigma(\alpha) = \sigma(\beta) + \sigma(\gamma) \equiv \beta + \gamma = \alpha \pmod{Q^{m+1}}.$$

□

Now we can prove the embedding results that we mentioned earlier.

Proposition 5.5.3. *E/V_1 can be embedded in the multiplicative group $(S/Q)^*$.*

Proof. Fix $\pi \in Q \setminus Q^2$. We will first show that for each $\sigma \in E$, there exists $\alpha \in S$ (depending on σ) such that

$$\sigma(\pi) \equiv \alpha\pi \pmod{Q^2}$$

and moreover α is uniquely determined mod Q. Since $\pi \in Q \setminus Q^2$, $\pi S = QI$ for some ideal I not divisible by Q. By the Chinese Remainder Theorem, there is a solution to

$$\begin{aligned} x &\equiv \sigma(\pi) \pmod{Q^2} \\ x &\equiv 0 \pmod{I}. \end{aligned}$$

But then $x \equiv \sigma(\pi) \equiv \pi \equiv 0 \pmod{Q}$ since $\sigma \in E$. Hence, $x \in Q \cap I = QI = \pi S$, so $x = \alpha\pi$ for some $\alpha \in S$. Thus, $\sigma(\pi) \equiv x \equiv \alpha\pi \pmod{Q^2}$. Moreover, if $\sigma(\pi) \equiv \alpha'\pi \pmod{Q^2}$ for some $\alpha' \in S$, then $\alpha'\pi \equiv \alpha\pi \pmod{Q^2}$. Since $\pi \in Q \setminus Q^2$, we must have $\alpha' \equiv \alpha \pmod{Q}$. Hence, α is unique mod Q. We will denote this element constructed as α_σ.

Let $\psi : E \to (S/Q)^*$ denote the map sending $\sigma \mapsto \overline{\alpha_\sigma}$ where the bar denotes the image under the quotient map by Q. We claim that ψ is a homomorphism. We have that

$$\begin{aligned} \sigma\tau(\pi) &\equiv \sigma(\alpha_\tau\pi) \pmod{Q^2} \\ &\equiv \sigma(\alpha_\tau)\sigma(\pi) \pmod{Q^2} \\ &\equiv \sigma(\alpha_\tau)\alpha_\sigma\pi \pmod{Q^2}. \end{aligned}$$

Now $\sigma(\alpha_\tau) \equiv \alpha_\tau \pmod{Q}$, so $(\sigma(\alpha_\tau) - \alpha_\tau)\alpha_\sigma\pi \in Q^2$. This gives us that

$$\sigma(\alpha_\tau)\alpha_\sigma\pi \equiv \alpha_\tau\alpha_\sigma\pi \pmod{Q^2}.$$

Hence,

$$\sigma\tau(\pi) \equiv \alpha_\sigma \alpha_\tau \pi \pmod{Q^2}.$$

By the uniqueness of $\alpha_{\sigma\tau}$, we must have $\alpha_{\sigma\tau} \equiv \alpha_\sigma \alpha_\tau \pmod{Q}$. Hence, $\psi(\sigma\tau) = \psi(\sigma)\psi(\tau)$, so ψ is a homomorphism. Moreover,

$$\begin{aligned}\ker \psi &= \{\sigma \in E \mid \alpha_\sigma \equiv 1 \pmod{Q}\} \\ &= \{\sigma \in E \mid \sigma(\pi) \equiv \pi \pmod{Q^2}\} \\ &= V_1,\end{aligned}$$

where the last equality follows from Prop. 5.5.2. By the First Isomorphism Theorem, we have an embedding $E/V_1 \hookrightarrow (S/Q)^*$. □

Proposition 5.5.4. *V_{m-1}/V_m can be embedded in the additive group S/Q for all $m \geq 2$.*

Proof. Fix $\pi \in Q \setminus Q^2$; then $\pi^m \in Q^m - Q^{m+1}$. For each $\sigma \in V_{m-1}$, we will show that there exists $\alpha \in S$ (depending on σ) such that $\sigma(\pi) \equiv \pi + \alpha\pi^m \pmod{Q^{m+1}}$ and moreover α is uniquely determined mod Q. Since $\pi \in Q \setminus Q^2$, $\pi S = QI$ for some ideal I not divisible by Q. By the Chinese Remainder Theorem, there is a solution to

$$\begin{aligned}x &\equiv \sigma(\pi) - \pi \pmod{Q^{m+1}} \\ x &\equiv 0 \pmod{I^m}.\end{aligned}$$

But then $x \equiv \sigma(\pi) - \pi \equiv 0 \pmod{Q^m}$ since $\sigma \in V_{m-1}$. Hence, $x \in Q^m \cap I^m = (QI)^m = (\pi)^m = (\pi^m)$. Therefore, there exists an element $\alpha \in S$ such that $x = \alpha\pi^m$. Thus, $\sigma(\pi) \equiv \pi + x \equiv \pi + \alpha\pi^m \pmod{Q^{m+1}}$. Moreover, if $\sigma(\pi) \equiv \pi + \alpha'\pi^m \pmod{Q^{m+1}}$ for some element $\alpha' \in S$, then $\alpha'\pi^m \equiv \alpha\pi^m \pmod{Q^{m+1}}$. Since $\pi^m \in Q^m - Q^{m+1}$, this implies $\alpha' \equiv \alpha \pmod{Q}$. Hence, α is unique mod Q. We will denote this element constructed as α_σ.

Let $\psi : V_{m-1} \to S/Q$ denote the map sending $\sigma \mapsto \overline{\alpha_\sigma}$ where the bar denotes the image under the quotient map by Q. We claim that ψ is a homomorphism. We have that

$$\begin{aligned}\sigma\tau(\pi) &\equiv \sigma(\pi + \alpha_\tau \pi^m) \pmod{Q^{m+1}} \\ &\equiv \sigma(\pi) + \sigma(\alpha_\tau)\sigma(\pi)^m \pmod{Q^{m+1}} \\ &\equiv \pi + \alpha_\sigma \pi^m + \sigma(\alpha_\tau)(\pi + \alpha_\sigma \pi^m)^m \pmod{Q^{m+1}} \\ &\equiv \pi + \alpha_\sigma \pi^m + \sigma(\alpha_\tau)\pi^m \pmod{Q^{m+1}}\end{aligned}$$

where the last equality holds only for $m \geq 2$. Now $\sigma(\alpha_\tau) \equiv \alpha_\tau \pmod{Q^m}$ since $\sigma \in V_{m-1}$, so $\sigma(\alpha_\tau) - \alpha_\tau \in Q^m$. Since $\pi \in Q$, it follows that $(\sigma(\alpha_\tau) - \alpha_\tau)\pi^m \in Q^{m+1}$. Hence, $\sigma(\alpha_\tau)\pi^m \equiv \alpha_\tau\pi^m \pmod{Q^{m+1}}$. Thus, $\sigma\tau(\pi) \equiv \pi + (\alpha_\sigma + \alpha_\tau)\pi^m \pmod{Q^{m+1}}$. By the uniqueness of $\alpha_{\sigma\tau}$, we have $\alpha_{\sigma\tau} \equiv \alpha_\sigma + \alpha_\tau \pmod{Q^{m+1}}$. Hence, $\psi(\sigma\tau) = \psi(\sigma) + \psi(\tau)$, so ψ is a homomorphism. Moreover,

$$\begin{aligned}\ker\psi &= \{\sigma \in V_{m-1} \mid \alpha_\sigma \equiv 0 \pmod{Q}\} \\ &= \{\sigma \in V_{m-1} \mid \sigma(\pi) \equiv \pi \pmod{Q^{m+1}}\} \\ &= V_m,\end{aligned}$$

where the last equality follows from Prop. 5.5.2. By the First Isomorphism Theorem, we have an embedding $V_{m-1}/V_m \hookrightarrow S/Q$. □

Because of these embeddings, we can deduce that V_1 is the Sylow p-subgroup of $E = V_0$ where $p = Q \cap \mathbb{Z}$. Consequently, all V_m for $m \geq 1$ are p-groups. First, we need the following lemma:

Lemma 5.5.5. *For sufficiently large m, V_m is trivial.*

Proof. For all $m \geq 1$, we have that $\bigcap_{k=0}^{\infty} Q^k \subseteq Q^m$. Thus, Q^m divides $\bigcap_{k=1}^{\infty} Q^k$. If $\bigcap_{k=1}^{\infty} Q^k \neq (0)$, then it has a unique prime factorization into prime ideals of S. This factorization would have to include Q^m for all $m \geq 1$, a contradiction. Thus, $\bigcap_{k=1}^{\infty} Q^k = (0)$.

Now suppose $\sigma \in \bigcap_{k=0}^{\infty} V_k$. Then for any $\alpha \in S$, $\sigma(\alpha) \equiv \alpha \pmod{Q^m}$ for all $m \geq 1$. Hence, $\sigma(\alpha) - \alpha \in \bigcap_{k=0}^{\infty} Q^k = (0)$. Hence, $\sigma(\alpha) - \alpha = 0$, so $\sigma(\alpha) = \alpha$ for all $\alpha \in S$. Consequently, $\sigma(\alpha) = \alpha$ for all $\alpha \in L$, so $\sigma = 1$. Hence, $\bigcap_{k=0}^{\infty} V_k = \{1\}$.

Since each V_m is finite, the descending chain

$$V_0 \supseteq V_1 \supseteq V_2 \supseteq \ldots$$

must be eventually constant. Then for m sufficiently large, $V_m = \bigcap_{k=0}^{\infty} V_k = \{1\}$. Hence for m sufficiently large, V_m is trivial. □

Proposition 5.5.6. *V_1 is the Sylow p-subgroup of E, where p is the prime of $\mathbb{Z}$ lying under Q.*

Proof. Suppose $|E| = p^k m$ where p does not divide m. We have that $|E/V_1|$ divides $|S/Q|-1$ by Prop. 5.5.3. But $|S/Q| - 1 = p^{f(Q \mid p)} - 1$ which is not divisible by p. Therefore, p does not divide $|E/V_1|$. Since $|E| = |V_1||E/V_1|$, it follows that p^k divides $|V_1|$.

Now for all $m \geq 2$, we have $|V_{m-1}|/|V_m| = p^l$ for some $l \geq 0$ by Prop. 5.5.4. It follows that if q is a prime not equal to p that divides $|V_1|$, then by induction q divides $|V_m|$ for all $m \geq 1$. But by Lemma 5.5.5, $|V_m| = 1$ for all m sufficiently large. It follows that p is the only prime dividing $|V_1|$, so $|V_1| = p^k$. Thus, V_1 is a Sylow p-subgroup of E. Since V_1 is normal in E, V_1 must be the unique Sylow p-subgroup of E. □

Example 5.5.7. Again returning to Example 5.1.1, let $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, $G = \mathrm{Gal}(L/\mathbb{Q})$, and $S = \mathcal{O}_L$. We have the prime factorization $3S = Q^2$ where $Q = (\sqrt{3})$. Let $D = D(Q \mid 3)$ and $E = E(Q \mid 3)$. We saw that $D = G$ and $E =< \sigma_1 >$ where σ_1 is the automorphism described in Example 5.1.1. Prop. 5.5.6 gives us that $V_1 = V_1(Q \mid 3)$ is the Sylow 3-subgroup of E. However, $|E| = 2$, so V_1 is the trivial group. Consequently, $V_m = V_m(Q \mid 3)$ is trivial for all $m \geq 1$. Hence, V_{m-1}/V_m can trivially be embedded in the additive group S/Q for $m \geq 2$. We have that $f = f(Q \mid 3) = 2$, so S/Q has degree 2 over $\mathbb{Z}/3\mathbb{Z}$. Thus, S/Q is the finite field of order 9, which means $(S/Q)^* \cong C_8$. Since $E/V_1 \cong E \cong C_2$, we see that E/V_1 can be embedded in $(S/Q)^*$.

In the case where D/V_1 is abelian, we can say more about the embedding $E/V_1 \hookrightarrow (S/Q)^*$. In this case, we in fact have an embedding $E/V_1 \hookrightarrow (R/P)^*$. For our purposes of proving the Kronecker-Weber Theorem, we will be considering only extensions where $G = \mathrm{Gal}(L/K)$ is abelian. In this case, D/V_1 is always abelian. Before we can prove this result, we need a technical lemma.

Lemma 5.5.8. *Fix $\pi \in Q \setminus Q^2$. Suppose $\sigma \in V_{m-1}$, $m \geq 1$, and $\sigma(\pi) \equiv \alpha\pi \pmod{Q^{m+1}}$ for some $\alpha \in S$. Then $\sigma(\beta) \equiv \alpha\beta \pmod{Q^{m+1}}$ for every $\beta \in Q$.*

Proof. First, suppose $\beta \in \pi S$. Then $\beta = \pi s$ for some $s \in S$. We have that

$$\sigma(\beta) = \sigma(\pi)\sigma(s) \equiv \sigma(s)\alpha\pi \pmod{Q^{m+1}}.$$

Now $\sigma(s) \equiv s \pmod{Q^m}$ since $\sigma \in V_{m-1}$, so $(\sigma(s) - s)\alpha\pi \in Q^{m+1}$. Thus, $\sigma(s)\alpha\pi \equiv s\alpha\pi \pmod{Q^{m+1}}$, so $\sigma(\beta) \equiv \alpha\beta \pmod{Q^{m+1}}$.

Now suppose $\beta \in Q$. We have that $\pi S = QI$ for some ideal I not divisible by Q. Pick $\gamma \in I \setminus Q$. Then $\gamma \notin Q$ but $\beta\gamma \in QI = \pi S$. By the previous case, we have

$$\begin{aligned}\sigma(\beta)(\sigma(\gamma) - \gamma) + \gamma\sigma(\beta) &= \sigma(\beta)\sigma(\gamma) \\ &= \sigma(\beta\gamma) \\ &\equiv \alpha\beta\gamma \pmod{Q^{m+1}}.\end{aligned}$$

But $\sigma(\gamma) \equiv \gamma \pmod{Q^m}$ and $\sigma(\beta) \equiv \beta \equiv 0 \pmod{Q}$, so $\sigma(\beta)(\sigma(\gamma) - \gamma) \equiv 0 \pmod{Q^{m+1}}$. Hence, $\gamma\sigma(\beta) \equiv \alpha\beta\gamma \pmod{Q^{m+1}}$. Since $\gamma \notin Q$, we must have $\sigma(\beta) \equiv \alpha\beta \pmod{Q^{m+1}}$. □

Now we can show that if D/V_1 is abelian, then there is an embedding $E/V_1 \hookrightarrow (R/P)^*$. We saw in Corollary 5.2.2 that $D/E \cong \overline{G} = \mathrm{Gal}(S/Q \;/\; R/P)$. Moreover, S/Q and R/P are finite fields, so $\overline{G}$ is cyclic with generator $\overline{\phi}$ where

$$\overline{\phi}(\overline{x}) = \overline{x}^{\|P\|}$$

for all $\overline{x} \in S/Q$. This corresponds via the isomorphism in Lemma 5.1.2 with an automorphism $\phi \in D$ (unique modulo E) such that

$$\phi(x) \equiv x^{\|P\|} \pmod{Q}$$

for all $x \in S$. We call such an automorphism ϕ **a Frobenius automorphism** of Q over P.

Proposition 5.5.9. *If D/V_1 is abelian, then $E/V_1 \hookrightarrow (R/P)^*$. In particular, E/V_1 is cyclic of order dividing $\|P\| - 1$.*

Proof. Fix $\pi \in Q \setminus Q^2$. Let $\alpha = \alpha_\sigma$ from the embedding in Prop. 5.5.3; that is, $\sigma(\pi) \equiv \alpha\pi \pmod{Q^2}$ and α is unique mod Q. Let ϕ be a Frobenius automorphism for Q over P. Since D/V_1 is abelian, for every $\sigma \in E$, we have that $\phi\sigma\phi^{-1}\sigma^{-1} \in V_1$. It follows that $\phi\sigma\phi^{-1}\sigma^{-1}(\sigma(\pi)) \equiv \sigma(\pi) \pmod{Q^2}$. Thus, $\phi\sigma\phi^{-1}(\pi) \equiv \sigma(\pi) \pmod{Q^2}$. We will show that

$$\phi\sigma\phi^{-1}(\pi) \equiv \alpha^{\|P\|}\pi \pmod{Q^2}.$$

From Lemma 5.5.8, we have that

$$\begin{aligned}\phi\sigma\phi^{-1}(\pi) &\equiv \phi(\alpha\phi^{-1}(\pi)) \pmod{Q^2} \\ &\equiv \phi(\alpha)\pi \pmod{Q^2}.\end{aligned}$$

Now $\phi(\alpha) \equiv \alpha^{\|P\|} \pmod{Q}$, so $(\phi(\alpha) - \alpha^{\|P\|})\pi \in Q^2$. Hence, $\phi(\alpha)\pi \equiv \alpha^{\|P\|}\pi \pmod{Q^2}$. Thus,

$$\phi\sigma\phi^{-1}(\pi) \equiv \alpha^{\|P\|}\pi \pmod{Q^2}.$$

Therefore, $\phi\sigma\phi^{-1}(\pi) \equiv \alpha^{\|P\|}\pi \pmod{Q^2}$. It follows that $\sigma(\pi) \equiv \alpha^{\|P\|}\pi \pmod{Q^2}$. But α is unique mod Q, so $\alpha^{\|P\|} \equiv \alpha \pmod{Q}$; that is, $\phi(\alpha) \equiv \alpha \pmod{Q}$.

Letting the bar now denote the image under the quotient by Q, we have that $\overline{\alpha}$ is fixed by $\overline{\phi}$. But $<\overline{\phi}>=\overline{G} = \mathrm{Gal}(S/Q \ / \ R/P)$, so $\overline{\alpha} \in R/P$. Since $\alpha \not\equiv 0 \pmod{Q}$, $\alpha \not\equiv 0 \pmod{P}$. Hence, $\overline{\alpha} \in (R/P)^*$. By the homomorphism given in Prop. 5.5.3, we have $E/V_1 \hookrightarrow (R/P)^*$. It follows that E/V_1 is cyclic of order dividing $|(R/P)^*| = \|P\| - 1$. □

5.6 Hilbert's Formula

We turn now to Hilbert's Formula, a relationship between the different and ramification groups. We will need Hilbert's Formula for our proof of the Kronecker-Weber Theorem in Chapter 6. First, we will need a couple of technical lemmas whose proofs we omit.

Lemma 5.6.1. *Let n be the degree of L over K. For each prime Q_i of S lying over P, fix a set $\{\beta_{i1}, ..., \beta_{if_i}\} \subseteq S$ corresponding to a basis for S/Q_i over R/P where $f_i = f(Q_i \mid P)$. For each $i = 1, ..., r$ and for each $j = 1, ..., e_i$ (where $e_i = e(Q_i \mid P)$) fix an element $\alpha_{ij} \in (Q_i^{j-1} \setminus Q_i^j) \cap \left(\bigcap_{h \neq i} Q_h^{e_h}\right)$. Consider the $n = \sum e_i f_i$ elements $\alpha_{ij}\beta_{ik}$ for $1 \leq i \leq r$ and $1 \leq j \leq e_i$. Then the corresponding elements in S/PS are linearly independent over R/P (we say that such elements are **independent mod P**).*

Lemma 5.6.2. *Let $n = [L : K]$ and $\alpha_1, ..., \alpha_n \in S$. If $\alpha_1, ..., \alpha_n$ are independent mod P, then $\alpha_1, ..., \alpha_n$ form a basis for L over K.*

Lemma 5.6.3. *Suppose Q is totally ramified over P. Let Q^k be the exact power of Q dividing* $\mathrm{diff}(S \mid R)$. *Then*

$$k = \sum_{m \geq 0} (|V_m| - 1).$$

Proof. Let $\pi \in Q \setminus Q^2$, and let f be the minimal polynomial for π over K. By Prop. 4.5.4, Q^k is the exact power of Q dividing $f'(\pi)S$. Since Q is totally ramified over P, we have that $G = E$. it follows from Lemma 5.5.5 that every element $\mathrm{id} \neq \sigma \in G$ lies in $V_{m-1} \setminus V_m$

for some $m \geq 1$. Suppose $\sigma \in V_{m-1} \setminus V_m$. Since $\sigma \in V_{m-1}$, $\pi - \sigma(\pi) \in Q^m$. Since $\sigma \notin V_m$, $\pi - \sigma(\pi) \notin Q^{m+1}$. Hence, $(\pi - \sigma(\pi))S$ is exactly divisible by Q^m.

By Lemma 5.6.1, we have that $\{1\}$ is a basis for S/Q over R/P and $\pi^{j-1} \in Q^{j-1} \setminus Q^j$ for $j = 1, ..., n$ where $n = [L : K] = e(Q|P)$, so $1, \pi, \pi^2, ..., \pi^{n-1}$ are independent mod P. By Lemma 5.6.2, $\{1, \pi, ..., \pi^{n-1}\}$ form a basis for L over K; that is, $L = K(\pi)$. It follows that $[L : K] = \deg(f)$ and $f(x) = \prod_{\sigma \in G}(x - \sigma(\pi))$. Therefore, $f'(\pi) = \prod_{\mathrm{id} \neq \sigma \in G}(\pi - \sigma(\pi))$. It follows that the exact power of Q dividing $f'(\pi)S$ is $k = \sum_{m \geq 1} m|V_{m-1} \setminus V_m|$. By Lemma 5.5.5, there exists $M \in \mathbb{N}$ such that $V_m = \{1\}$ for all $m \geq M$. Then $k = \sum_{m=1}^{M} m|V_{m-1} \setminus V_m|$. Since $V_m \subseteq V_{m-1}$, we have that $|V_{m-1} \setminus V_m| = |V_{m-1}| - |V_m|$. Hence,

$$\begin{aligned} k &= \sum_{m=1}^{M} (m|V_{m-1}| - m|V_m|) \\ &= \sum_{m=1}^{M} (m - (m-1))|V_{m-1}| - M|V_M| \\ &= \sum_{m=1}^{M} |V_{m-1}| - M|V_M| \\ &= \sum_{m=1}^{M} (|V_{m-1}| - 1) \\ &= \sum_{m \geq 0} (|V_m| - 1). \end{aligned}$$

□

Theorem 5.6.4 (Hilbert's Formula)**.** *Let Q^k be the exact power of Q dividing* $\mathrm{diff}(S \mid R)$. *Then*

$$k = \sum_{m \geq 0} (|V_m| - 1).$$

Proof. We have that $\mathrm{diff}(S \mid R) = \mathrm{diff}(S \mid S^E)\,\mathrm{diff}(S^E \mid R)S$ by Prop. 4.5.3. We have that P is unramified in S^E, so by Theorem 4.5.2, Q^E does not divide $\mathrm{diff}(S^E \mid R)$. Thus, Q does not divide $\mathrm{diff}(S^E \mid R)S$. It follows that k is the exact power of Q dividing $\mathrm{diff}(S \mid S^E)$. We have that Q is totally ramified over Q^E, so by Lemma 5.6.3

$$k = \sum_{m \geq 0} \big(|V_m(Q \mid Q^E)| - 1\big).$$

But

$$\begin{aligned} V_m(Q \mid Q^E) &= \{\sigma \in \mathrm{Gal}(L/L^E) \mid \sigma(\alpha) \equiv \alpha \pmod{Q^{m+1}}\ \forall \alpha \in S\} \\ &= \{\sigma \in E \mid \sigma \in V_m = V_m(Q \mid P)\} \\ &= E \cap V_m \\ &= V_m. \end{aligned}$$

Hence, $k = \sum_{m \geq 0} (|V_m| - 1)$. □

Chapter 6
The Kronecker-Weber Theorem

6.1 Introduction

We now turn to proving the Kronecker-Weber Theorem:

Theorem (Kronecker-Weber). *Every finite, abelian extension K of $\mathbb{Q}$ is contained in a cyclotomic field.*

Our proof is based on the one presented in [2], and it relies on the following result:

Theorem 6.1.1 (Minkowski). *Let K be a number field not equal to $\mathbb{Q}$ and let $R = \mathcal{O}_K$. Then $|\Delta(R)| > 1$.*

By Theorem 4.4.1, an immediate corollary is the following:

Corollary 6.1.2. *Let K be a number field distinct from $\mathbb{Q}$, and let $R = \mathcal{O}_K$. Then some prime $p \in \mathbb{Z}$ ramifies in R.*

The following result gives us an embedding of Galois groups that will be useful in the course of the proof.

Lemma 6.1.3. *Suppose K and L are normal extensions of $\mathbb{Q}$. Then $\mathrm{Gal}(KL/\mathbb{Q})$ can be embedded into $\mathrm{Gal}(K/\mathbb{Q}) \times \mathrm{Gal}(L/\mathbb{Q})$.*

Proof. We have that KL is normal over $\mathbb{Q}$ since both K and L are. For any $\sigma \in \mathrm{Gal}(KL/\mathbb{Q})$, consider the restriction to K, $\sigma\big|_K$. Since KL is normal over K, $\sigma(K) = K$. Hence, $\sigma|_K$ is an automorphism of K that fixes $\mathbb{Q}$ pointwise, so $\sigma\big|_K \in \mathrm{Gal}(K/\mathbb{Q})$. Similarly, $\sigma\big|_L \in \mathrm{Gal}(L/\mathbb{Q})$. Consider the homomorphism $\psi : \mathrm{Gal}(KL/\mathbb{Q}) \to \mathrm{Gal}(K/\mathbb{Q}) \times \mathrm{Gal}(L/\mathbb{Q})$ mapping $\sigma \mapsto (\sigma\big|_K, \sigma\big|_L)$. Then the kernel is

$$\begin{aligned}
\ker\psi &= \{\sigma \in \mathrm{Gal}(KL/\mathbb{Q}) \mid \sigma\big|_K = \mathrm{id}, \sigma\big|_L = \mathrm{id}\} \\
&= \{\sigma \in \mathrm{Gal}(KL/\mathbb{Q}) \mid \sigma \text{ fixes } K \text{ and } L \text{ pointwise}\} \\
&\subseteq \{\sigma \in \mathrm{Gal}(KL/\mathbb{Q}) \mid \sigma \text{ fixes } KL \text{ pointwise}\} \\
&= \{\mathrm{id}\}.
\end{aligned}$$

Hence, $\ker\psi = \{\mathrm{id}\}$ so ψ is injective. Thus, we have an embedding

$$\mathrm{Gal}(KL/\mathbb{Q}) \hookrightarrow \mathrm{Gal}(K/\mathbb{Q}) \times \mathrm{Gal}(L/\mathbb{Q}).$$

□

6.2 Special Case: The field K has prime power degree p^m over $\mathbb{Q}$ and $p \in \mathbb{Z}$ is the only ramified prime

We will first prove the Kronecker-Weber Theorem for a number of special cases. Our first special case will be when the degree of K over $\mathbb{Q}$ is a prime power p^m and p is the only prime of $\mathbb{Z}$ that ramifies in $R = \mathcal{O}_K$. First, we consider when $p = 2$. For easier readability, we will let $\omega(m) = \omega_m$.

Proposition 6.2.1. *Suppose K is an abelian extension of $\mathbb{Q}$ of degree 2^m for some positive integer m, and that 2 is the only prime of $\mathbb{Z}$ that ramifies in $R = \mathcal{O}_K$. Then K is contained in the 2^{m+2}-th cyclotomic field.*

Proof. First, suppose $m = 1$. We have that $K = \mathbb{Q}(\sqrt{n})$ for some squarefree integer n. As we saw in Example 3.3.10,

$$\Delta(\mathcal{O}_K) = \begin{cases} 4n & \text{if } n \equiv 2 \text{ or } 3 \pmod 4 \\ n & \text{if } n \equiv 1 \pmod 4. \end{cases}$$

Moreover, $|\Delta(\mathcal{O}_K)|$ must be a power of 2 in order for 2 to be the only ramified prime. In any case, we must have that n is a power of 2. If $n \equiv 1 \pmod 4$, then $n = 1$ is the only possibility; in this case, $\mathbb{Q}(\sqrt{n}) = \mathbb{Q}$ is not a quadratic extension of $\mathbb{Q}$. If $n \equiv 3 \pmod 4$, then $n = -1$ is the only possibility; in this case, we obtain $K = \mathbb{Q}(i)$. If $n \equiv 2 \pmod 4$, then since n is a squarefree power of 2, we must have $n = \pm 2$; in these cases, we obtain $K = \mathbb{Q}(\sqrt{2})$ or $\mathbb{Q}(\sqrt{-2})$. Thus, $K = \mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2})$, or $\mathbb{Q}(\sqrt{-2})$. In all cases, we have that $K \subseteq \mathbb{Q}(\omega_8)$ since $i = \omega_8^2$, $\sqrt{2} = \omega_8 + \omega_8^{-1}$, and $\sqrt{-2} = \omega_8 - \omega_8^{-1}$.

Now suppose $m > 1$. Consider $K \cap \mathbb{R}$. We have that either $K \subseteq \mathbb{R}$, or complex conjugation ψ is an element of $\mathrm{Gal}(K/\mathbb{Q})$. For the first case, $K \cap \mathbb{R} = K$; for the second, $K \cap \mathbb{R} = K^{<\psi>}$ has degree 2^{m-1} over $\mathbb{Q}$. In either case, there is a subfield of K' of $K \cap \mathbb{R}$ of degree 2 over $\mathbb{Q}$ since $\mathrm{Gal}(K \cap \mathbb{R}/\mathbb{Q})$ is a 2-group, and so it must have a subgroup of index 2. Now K' must have some prime that is ramified by Minkowski's Theorem since $K' \neq \mathbb{Q}$; since 2 is the only ramified prime in K, 2 must be the only ramified prime in K'. By the previous case, $K' = \mathbb{Q}(\sqrt{2}), \mathbb{Q}(i)$, or $\mathbb{Q}(\sqrt{-2})$. Since $K' \subseteq \mathbb{R}$, we must have $K' = \mathbb{Q}(\sqrt{2})$. Thus, $\mathbb{Q}(\sqrt{2}) \subseteq K$.

Set $L = \mathbb{R} \cap \mathbb{Q}(\omega(2^{m+2}))$. We have that 2 is totally ramified in $\mathbb{Q}(\omega(2^{m+2}))$, so 2 is totally ramified in L. We have that L has degree 2^m over $\mathbb{Q}$, so by the previous argument

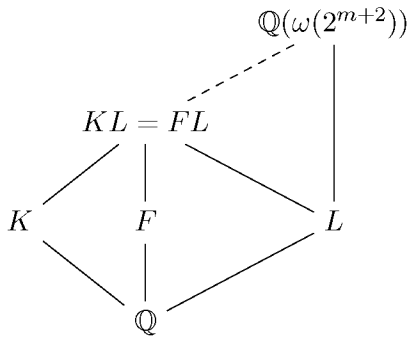


Figure 6.1. The tower of fields in the proof of Prop. 6.2.1.

$\mathbb{Q}(\sqrt{2}) \subseteq L$. Now suppose K' is a quadratic subfield of L. Then 2 must be totally ramified in K'. Then we must have $K' = \mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(i)$, or $\mathbb{Q}(\sqrt{-2})$. But $K' \subseteq L \subseteq \mathbb{R}$, so it must be the case that $K' = \mathbb{Q}(\sqrt{2})$. Hence, $\mathbb{Q}(\sqrt{2})$ is the unique quadratic subfield of L. By the fundamental theorem of finitely-generated abelian groups, $\mathrm{Gal}(L/\mathbb{Q}) \cong \mathbb{Z}/2^{k_1}\mathbb{Z} \times ... \times \mathbb{Z}/2^{k_r}\mathbb{Z}$ for some nonnegative integers $k_1, ..., k_r$. Since $\mathbb{Q}(\sqrt{2})$ is the unique quadratic subfield of L, it follows that $\mathrm{Gal}(L/\mathbb{Q}(\sqrt{2}))$ is the unique subgroup of $\mathrm{Gal}(L/\mathbb{Q})$ of order 2^{m-1}. It follows that $\mathrm{Gal}(L/\mathbb{Q}) \cong \mathbb{Z}/2^m\mathbb{Z}$. Thus, $\mathrm{Gal}(L/\mathbb{Q})$ is cyclic.

Let σ be a generator of $\mathrm{Gal}(L/\mathbb{Q})$ and extend σ to an automorphism τ of KL. Let F denote the fixed field of τ. We have that

$$\begin{aligned} F \cap L &= \{\alpha \in L \mid \tau(\alpha) = \alpha\} \\ &= \{\alpha \in L \mid \sigma(\alpha) = \alpha\} \\ &= L^{\mathrm{Gal}(L/\mathbb{Q})} \\ &= \mathbb{Q}. \end{aligned}$$

Moreover, we have that $[F : \mathbb{Q}]$ is a power of 2 since $[KL : \mathbb{Q}]$ is. Furthermore, 2 is the only ramified prime in KL by Prop. 5.3.2, so if $F \neq \mathbb{Q}$ then 2 must be the only ramified prime in F. If $[F : \mathbb{Q}] > 2$, then we must have that $\mathbb{Q}(\sqrt{2}) \subseteq F$. But then $\mathbb{Q}(\sqrt{2}) \subseteq F \cap L$, which is a contradiction. Thus, $[F : \mathbb{Q}] \leq 2$. If $[F : \mathbb{Q}] = 2$, then we must have $F = \mathbb{Q}(i)$ or $\mathbb{Q}(\sqrt{-2})$. Thus, either $F = \mathbb{Q}, \mathbb{Q}(i)$, or $\mathbb{Q}(\sqrt{-2})$. In any case, $F \subseteq \mathbb{Q}(\omega_8) \subseteq \mathbb{Q}(\omega_{2^{m+2}})$. We will show that $FL = KL$. It will then follow that $K \subseteq KL = FL \subseteq \mathbb{Q}(\omega_{2^{m+2}})$.

We have that $FL \subseteq KL$ since $F, L \subseteq KL$. Moreover from Lemma 6.1.3, we have

an embedding $\mathrm{Gal}(KL/\mathbb{Q}) \hookrightarrow \mathrm{Gal}(K/\mathbb{Q}) \times \mathrm{Gal}(L/\mathbb{Q})$ via the map $\psi \mapsto (\psi|_K, \psi|_L)$. Let $a = |\tau\big|_K|$ and $b = |\tau\big|_L|$. Then $|(\tau\big|_K, \tau\big|_L)| = \mathrm{lcm}(a,b)$. Since both $\mathrm{Gal}(K/\mathbb{Q})$ and $\mathrm{Gal}(L/\mathbb{Q})$ have order 2^m, it must be the case that a and b both divide 2^m. Moreover, $b = |\tau\big|_L| = |\sigma| = 2^m$ since $< \sigma >= \mathrm{Gal}(L/\mathbb{Q})$, so $\mathrm{lcm}(a,b) = 2^m$. Thus, $|\tau| = |(\tau\big|_K, \tau\big|_L)| = 2^m$. Consequently,

$$[KL : F] = |\operatorname{Gal}(KL/F)| = | < \tau > | = 2^m = [L : \mathbb{Q}].$$

It follows that

$$\begin{aligned} [KL : \mathbb{Q}] &= [KL : F][F : \mathbb{Q}] \\ &= [L : \mathbb{Q}][F : \mathbb{Q}] \\ &= [FL : \mathbb{Q}] \end{aligned}$$

where the last equality holds since $F \cap L = \mathbb{Q}$. Thus, $KL = FL$, and so $K \subseteq \mathbb{Q}(\omega_{2^{m+2}})$. $\square$

We will next turn to the case when the degree of K over $\mathbb{Q}$ is an odd prime power p^m and p is the only prime of $\mathbb{Z}$ that ramifies in $R = \mathcal{O}_K$. First, we will need some lemmas.

Lemma 6.2.2. *Suppose K is an abelian extension of $\mathbb{Q}$ with odd prime degree p, and that p is the only prime of $\mathbb{Z}$ that ramifies in $R = \mathcal{O}_K$. Let P be a prime of R lying over p. Then* $\mathrm{diff}(R \mid \mathbb{Z}) = P^{2(p-1)}$.

Proof. Since K is a normal extension of $\mathbb{Q}$, all primes of R lying over p must have the same ramification index. It follows that P is ramified over p. Since $e(P \mid p) > 1$ and divides $[K : \mathbb{Q}] = p$, we must have $e(P \mid p) = p$. Fix $\pi \in P \setminus P^2$. Then $\pi \notin \mathbb{Q}$ since $\pi \notin P^p$. Since $\mathbb{Q} \subsetneq \mathbb{Q}(\pi) \subseteq K$ and K has degree p over $\mathbb{Q}$, we must have that $\mathbb{Q}(\pi)$ has degree p over $\mathbb{Q}$. Let

$$f(x) = x^p + a_1 x^{p-1} + ... + a_p$$

be the minimal polynomial for π over $\mathbb{Q}$. Since π is an algebraic integer, all $a_i \in \mathbb{Z}$ by Prop. 3.1.4. Let P^k be the exact power of P dividing $\mathrm{diff}(R \mid \mathbb{Z})$. By Hilbert's formula,

$$k = \sum_{m \geq 0} \left(|V_m| - 1 \right).$$

We have that $|V_m|$ divides $|V_0| = e(P \mid p) = p$ for $m \geq 0$. Thus, for $m \geq 0$ either $|V_m| - 1 = p - 1$ or 0 . Hence, k is a multiple of $p - 1$.

By Prop. 4.5.4, P^k is the exact power of P dividing $f'(\pi)$. We claim that k is the minimum of the exponents of P dividing each term of $f'(\pi) = p\pi^{p-1} + ... + a_{p-1}$. Since $P \cap \mathbb{Z} = p\mathbb{Z}$ and $pR = P^p$, we have that the exact power of P dividing $a_i(p-i)$ is a multiple of p for all $0 \leq i \leq p-1$. Since $\pi \in P \setminus P^2$, the exact power of P dividing π^{p-i-1} is $p-i-1$. Hence, the exact power of P dividing $a_i(p-i)\pi^{p-i-1}$ is congruent to $p-i-1$ mod p. Thus all of the exponents of P for the terms of $f'(\pi)$ are incongruent mod p, and so they must all be distinct. Let l be the minimum of these exponents, and let $a_j(p-j)\pi^{p-j-1}$ be the unique term whose exponent of P is l. Clearly, $k \geq l$ since P^l divides each term of $f'(\pi)$, and hence must divide $f'(\pi)$ itself. Suppose $k > l$. We have that

$$a_j(p-j)\pi^{p-j-1} = f'(\pi) - \sum_{i \neq j} a_i(p-i)\pi^{p-i-1}.$$

The exponent of P dividing each term of the right-hand side is greater than l. It follows that some power greater than l of P divides $a_j(p-j)\pi^{p-j-1}$, which is a contradiction. Hence, $k = l$ is the minimum exponent of P dividing the terms of $f'(\pi)$.

We claim that all a_i are divisible by p. Since $e(P \mid p) = p = [K : \mathbb{Q}]$, we have that $f(P \mid p) = 1$. Thus, $\{1\}$ is a basis for R/P over $\mathbb{Z}/p\mathbb{Z}$. We have that $\pi^{j-1} \in P^{j-1} - P^j$. By Lemma 5.6.1, $1, \pi, ..., \pi^{p-1}$ are independent mod p. Now $\pi^p \in P^p = pR$, so $0 = f(\pi) \equiv a_1\pi^{p-1} + ... + a_p \pmod{pR}$. Since $1, \pi, ..., \pi^{p-1}$ are independent mod p, it follows that $a_1 \equiv ... \equiv a_p \equiv 0 \pmod{p}$. Thus, all a_i are divisible by p.

It follows that P^p divides all terms of $f'(\pi)$. Hence, $k \geq p$. Moreover, we have that P^{2p-1} is the exact power of P dividing $p\pi^{p-1}$, the leading term of $f'(\pi)$, so $k \leq 2p-1$. Since $p \geq 3$, we have that $p-1 < p \leq k \leq 2p-1 < 3(p-1)$. Since k is a multiple of $p-1$, the only possibility is that $k = 2(p-1)$. Thus, the exact power of P dividing $\mathrm{diff}(R \mid \mathbb{Z})$ is $2(p-1)$.

Now suppose Q is another prime ideal of R dividing $\mathrm{diff}(R \mid \mathbb{Z})$. Let q be the prime of $\mathbb{Z}$ lying under Q. Since p is totally ramified in R and $Q \neq P$, we must have that $q \neq p$. By Theorem 4.5.2, q is ramified in R. However, p is the only prime of $\mathbb{Z}$ ramified in R. Thus, no other prime ideal of R divides $\mathrm{diff}(R \mid \mathbb{Z})$. Therefore, $\mathrm{diff}(R \mid \mathbb{Z}) = P^{2(p-1)}$. □

Lemma 6.2.3. *Suppose K is an abelian extension of $\mathbb{Q}$ of degree p^2 for some odd prime p, and that p is the only prime of $\mathbb{Z}$ that ramifies in $R = \mathcal{O}_K$. Then $G = \mathrm{Gal}(K/\mathbb{Q})$ has a unique subgroup of order p.*

Proof. Let P be a prime of K lying over p. Let $E = E(P \mid p)$ and consider the inertia field K^E. Let $P' = P \cap K^E$. Then $e(P' \mid p) = 1$, and since $E \triangleleft \mathrm{Gal}(K/\mathbb{Q})$ we must have that p is unramified in K^E. However, all primes of $\mathbb{Z}$ not equal to p are unramified in K, and so they must be unramified in K^E. Hence, no prime of $\mathbb{Z}$ is ramified in K^E. It follows from Minkowski's Theorem that $K^E = \mathbb{Q}$. Hence, $e(P \mid p) = [K : K^E] = [K : \mathbb{Q}]$, so P is totally ramified over p. Thus, $|E(P \mid p)| = e(P \mid p) = [K : \mathbb{Q}] = p^2$. By Prop. 5.5.6, V_1 is the Sylow p-subgroup of $E(P \mid p)$. Thus, $V_1 = E(P \mid p)$ and $|V_1| = p^2$. Let $V_r = V_r(P \mid p)$ be the first ramification group having order less than p^2. Then $r > 1$. We have from Prop. 5.5.4 an embedding $V_{r-1}/V_r \hookrightarrow R/P$. Hence, $|V_{r-1}/V_r|$ divides $|R/P| = p^{f(P \mid p)}$. Since P is totally ramified over p, $f(P|p) = 1$. Hence, $|R/P| = p$ and so $|V_{r-1}/V_r| = 1$ or p. But $|V_{r-1}| = p^2$ and $|V_r| < p^2$, so $|V_{r-1}/V_r| > 1$. Thus, $|V_{r-1}/V_r| = p$, and therefore $|V_r| = p$. Hence, V_r is a subgroup of G of order p. We will show that it is the unique subgroup of G of order p.

Let H be any subgroup of G having order p, and let K^H be the fixed field of H. By Prop. 4.5.3, we have that

$$\mathrm{diff}(R \mid \mathbb{Z}) = \mathrm{diff}(R \mid R^H)(\mathrm{diff}(R^H \mid \mathbb{Z})R)$$

where $R^H = \mathcal{O}_{K^H}$. Since $K^H \neq \mathbb{Q}$, some prime of $\mathbb{Z}$ is ramified in R^H by Minkowski's Theorem; since p is the only prime ramified in R, p must be the only ramified prime in R^H. Moreover, $[K^H : \mathbb{Q}] = p^2/p = p$. By Lemma 6.2.2, $\mathrm{diff}(R^H \mid \mathbb{Z}) = (P^H)^{2(p-1)}$. Since P is totally ramified over p, P must be totally ramified over P^H. Then $e(P \mid P^H) = [K : K^H] = p$ and $P^H R = P^p$. Thus, $\mathrm{diff}(R^H \mid \mathbb{Z})R = P^{2(p-1)p}$ and so

$$\mathrm{diff}(R \mid \mathbb{Z}) = \mathrm{diff}(R \mid R^H)P^{2(p-1)p}.$$

This shows that $\mathrm{diff}(R \mid R^H)$ is independent of H. We will show that the exponent of P in $\mathrm{diff}(R \mid R^H)$ is strictly maximized when $H = V_r$. Thus, if $H \neq V_r$, then $\mathrm{diff}(R \mid R^H) \neq \mathrm{diff}(R \mid R^{V_r})$. Since $\mathrm{diff}(R \mid R^H)$ is independent of H, it then follows that V_r must be the unique subgroup of G of order p.

By Hilbert's formula, the exact power of P dividing $\mathrm{diff}(R \mid R^H)$ is

$$k = \sum_{m \geq 0} \left(|V_m(P \mid P^H)| - 1 \right).$$

We have that

$$\begin{aligned} V_m(P \mid P^H) &= \{\sigma \in \mathrm{Gal}(K/K^H) \mid \sigma(\alpha) \equiv \alpha \pmod{P^{m+1}}\ \forall \alpha \in R\} \\ &= \{\sigma \in H \mid \sigma \in V_m(P \mid p)\} \\ &= H \cap V_m \end{aligned}$$

where $V_m = V_m(P \mid p)$. Hence, $|V_m(P \mid P^H)|$ is maximized when $V_m \subseteq H$ or $H \subseteq V_m$. For $m \leq r$, we have that $|V_m| \geq |H|$. Hence, $|V_m(P \mid P^H)|$ is maximized for all $m \leq r$ precisely when $H \subseteq V_r \subseteq ... \subseteq V_0$. Similarly, for $m \geq r$, we have that $|V_m| \leq |H|$. Hence, $|V_m(P \mid P^H)|$ is maximized for all $m \geq r$ precisely when $H \supseteq V_r \supseteq V_{r+1} \supseteq ....$ It follows that k is maximized precisely when $H = V_r$. Therefore, V_r must be the only subgroup of order p in G. □

Lemma 6.2.4. *Suppose K is an abelian extension of $\mathbb{Q}$ with odd prime degree p, and that p is the only prime of $\mathbb{Z}$ that ramifies in $\mathcal{O}_K$. Then K is the unique subfield of the p^2-th cyclotomic field having degree p over $\mathbb{Q}$.*

Proof. Suppose we have distinct fields K and L of degree p over $\mathbb{Q}$ with p the only ramified prime in each. Consider the composite field KL. Since $K \cap L = \mathbb{Q}$, we have that $[KL : \mathbb{Q}] = [K : \mathbb{Q}][L : \mathbb{Q}] = p^2$. We have that for any prime $q \neq p$ of $\mathbb{Z}$ that q is unramified in both K and L. By Prop. 5.3.2, q must be unramified in KL. Hence KL has degree p^2 over $\mathbb{Q}$ with p being the only ramified prime. By Lemma 6.2.3 and the Galois correspondence theorem, there is a unique subfield of KL having index p (and hence degree p over $\mathbb{Q}$). But K and L are distinct subfields of KL having degree p over $\mathbb{Q}$, which is a contradiction. Thus, there is at most one field K of degree p over $\mathbb{Q}$ in which p is the only ramified prime.

Since $\varphi(p^2) = p(p-1)$, there is a subfield L of the p^2-th cyclotomic field $\mathbb{Q}(\omega_{p^2})$ having degree p over $\mathbb{Q}$. Moreover, since p is the only ramified prime in $\mathbb{Q}(\omega_{p^2})$, p can be the only ramified prime in L. Since p is totally ramified in $\mathbb{Q}(\omega_{p^2})$, p must be totally ramified in L. It follows that $K = L$ is the unique abelian extension of $\mathbb{Q}$ of degree p with p being the only ramified prime. □

Proposition 6.2.5. *Suppose K is an abelian extension of $\mathbb{Q}$ with odd prime power degree p^m for some positive integer m, and that p is the only prime of $\mathbb{Z}$ that ramifies in $R = \mathcal{O}_K$. Then K is the unique subfield of the p^{m+1}-th cyclotomic field having degree p^m over $\mathbb{Q}$.*

Proof. We have that $\mathrm{Gal}(\mathbb{Q}(\omega_{p^{m+1}})/\mathbb{Q}) \cong (\mathbb{Z}/p^{m+1}\mathbb{Z})^*$ is cyclic. Let L be the unique subfield of the p^{m+1}-th cyclotomic field having degree p^m over $\mathbb{Q}$. Then $\mathrm{Gal}(L/\mathbb{Q})$ is cyclic; let σ be a generator. Extend σ to an automorphism τ of KL, and let F be the fixed field of τ. We have that

$$\begin{aligned} F \cap L &= \{\alpha \in L \mid \tau(\alpha) = \alpha\} \\ &= \{\alpha \in L \mid \sigma(\alpha) = \alpha\} \\ &= L^{<\sigma>} \\ &= L^{\mathrm{Gal}(L/\mathbb{Q})} \\ &= \mathbb{Q}. \end{aligned}$$

Moreover, we have that $[F : \mathbb{Q}]$ is a power of p since $[KL : \mathbb{Q}]$ is. Since p is the only ramified prime in K and L, by Prop. 5.3.2, p is the only ramified prime in KL. Hence, p is the only prime that might ramify in F. Suppose $F \neq \mathbb{Q}$. Then p must be ramified in F. In this case, F must contain a subfield F' of degree p over $\mathbb{Q}$ with p being the only ramified prime in F'. We have by Lemma 6.2.4 that F' is the unique subfield of the p^2-th cyclotomic field. Therefore $F' \subseteq L$, so $F' \subseteq F \cap L$. But $F \cap L = \mathbb{Q}$. It follows that $F = \mathbb{Q}$.

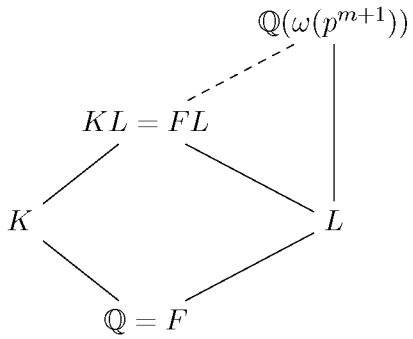


Figure 6.2. The tower of fields in the proof of Prop. 6.2.5.

From Lemma 6.1.3, we have an embedding $\mathrm{Gal}(KL/\mathbb{Q}) \hookrightarrow \mathrm{Gal}(K/\mathbb{Q}) \times \mathrm{Gal}(L/\mathbb{Q})$ via the map $\psi \mapsto (\psi\big|_K, \psi\big|_L)$. Let $a = |\tau\big|_K|$ and $b = |\tau\big|_L|$. Then $|\tau| = |(\tau\big|_K, \tau\big|_L)| = \mathrm{lcm}(a, b)$. Since $|\mathrm{Gal}(K/\mathbb{Q})| = p^m$, $a \,\Big|\, p^m$. Moreover,

$$b = |\tau\big|_L| = |\sigma| = |\mathrm{Gal}(L/\mathbb{Q})| = p^m.$$

Hence, $|\tau| = \text{lcm}(a, b) = p^m$.

We have that $F = \mathbb{Q}$, and so $[KL : \mathbb{Q}] = [KL : F]$. But $[KL : F] = |\text{Gal}(KL/F)| = |\tau| = p^m$, and so $[KL : \mathbb{Q}] = p^m$. Therefore, $L \subseteq KL$ and $[KL : \mathbb{Q}] = p^m = [L : \mathbb{Q}]$. It follows that $L = KL$. Therefore, $K \subseteq KL = L$. Since $[K : \mathbb{Q}] = p^m = [L : \mathbb{Q}]$, we must have $K = L$. Thus, K is the unique subfield of the p^{m+1}-th cyclotomic field having degree p^m over $\mathbb{Q}$. □

6.3 Special Case: The field K has prime power degree over $\mathbb{Q}$

We will next show that any abelian extension K of $\mathbb{Q}$ of prime power degree is contained in a cyclotomic field. We will prove the result by induction with Propositions 6.2.1 and 6.2.5 serving as the base case. The result will follow easily once we have established the following lemma.

Lemma 6.3.1. *Suppose K is an abelian extension of $\mathbb{Q}$ with prime power degree p^m, and let $q \neq p$ be a prime that ramifies in $R = \mathcal{O}_K$. Then there exists a field K' such that the following hold:*

(1) q is unramified in $\mathcal{O}_{K'}$ and every prime of $\mathbb{Z}$ which is unramified in $\mathcal{O}_K$ is also unramified in $\mathcal{O}_{K'}$.

(2) K' has degree p^k over $\mathbb{Q}$ where $k \leq m$.

(3) If K' is contained in the d-th cyclotomic field where q does not divide d, then K is contained in the dq-th cyclotomic field.

Proof. Fix a prime Q of R lying over q, and set $e = e(Q \mid q)$. Since K is normal over $\mathbb{Q}$, $e \Big| [K : \mathbb{Q}] = p^m$. Thus, e is a power of p. By Prop. 5.5.6, $V_1(Q \mid q)$ is the Sylow q-subgroup of $E(Q \mid q)$. But $|E(Q \mid q)| = e$, so it follows that $V_1(Q \mid q)$ is trivial. We have that $D(Q \mid q)/V_1(Q \mid q)$ is abelian, so by Prop. 5.5.9, $E(Q \mid q)/V_1(Q \mid q)$ is cyclic of order dividing $q - 1$. But $V_1(Q \mid q) = \{1\}$, so $E(Q \mid q)/V_1(Q \mid q) \cong E(Q \mid q)$. Hence, $|E(Q \mid q)| = e$ divides $q - 1$. It follows that the q-th cyclotomic field has a unique subfield L of degree e over $\mathbb{Q}$. Let W be a prime of the q-th cyclotomic field $\mathbb{Q}(\omega_q)$ lying over q. We have that q is totally ramified in $\mathbb{Q}(\omega_q)$. Hence, $f(W \mid q) = 1$ and there is one prime of

$\mathbb{Q}(\omega_q)$ lying over q. It follows that $f(W \cap L \mid q) = 1$ and there is one prime of L lying over q, so $e(W \cap L \mid q) = e$. Hence, q is totally ramified in L.

Let U be a prime of KL lying over Q, and let K' denote the inertia field $(KL)^{E(U \mid q)}$. From Lemma 6.1.3, we have that $\mathrm{Gal}(KL/\mathbb{Q}) \hookrightarrow \mathrm{Gal}(K/\mathbb{Q}) \times \mathrm{Gal}(L/\mathbb{Q})$ via the map $\sigma \mapsto (\sigma|_K, \sigma|_L)$. Hence, $\mathrm{Gal}(KL/\mathbb{Q})$ is abelian. We have that $D(U \mid q)$ and $E(U \mid q)$ are normal subgroups of $\mathrm{Gal}(KL/\mathbb{Q})$ (since $\mathrm{Gal}(KL/\mathbb{Q})$ is abelian). By Corollary 5.2.3, q is unramified in $K' = (KL)^{E(U \mid q)}$. Moreover, for any prime $u \in \mathbb{Z}$ which is unramified in K, we have that u is unramified in the q-th cyclotomic field and hence unramified in L as well. By Prop. 5.3.2, u is unramified in KL. Therefore, u must be unramified in K'. Therefore, q is unramified in K' and every prime of $\mathbb{Z}$ which is unramified in K is also unramified in KL, hence also in K'. This establishes (1).

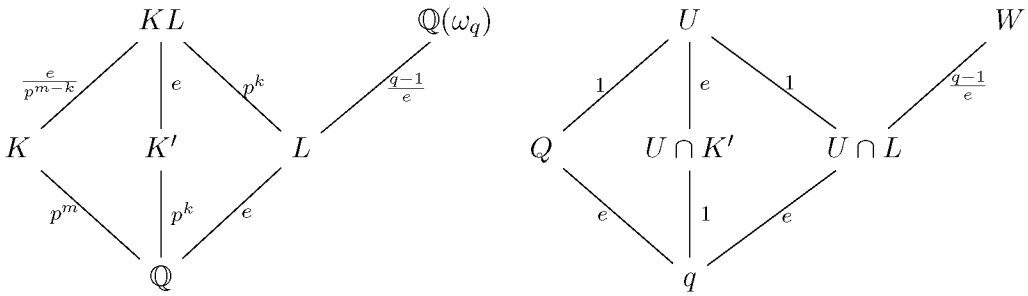


Figure 6.3. Left: The tower of fields in the proof of Prop. 6.3.1 along with the corresponding degrees; Right: The corresponding tower of primes lying over q and their ramification indices.

We claim that $[KL : K'] = e(U \mid q) = e$. Considering again the embedding $\mathrm{Gal}(KL/\mathbb{Q}) \hookrightarrow \mathrm{Gal}(K/\mathbb{Q}) \times \mathrm{Gal}(L/\mathbb{Q})$, suppose $\sigma \in E(U \mid q)$. Then for all $\alpha \in \mathcal{O}_{KL}$, $\sigma(\alpha) \equiv \alpha \pmod{U}$. Restricting to K, we have that for all $\alpha \in \mathcal{O}_K$, $\sigma\big|_K(\alpha) \equiv \alpha \pmod{U \cap K}$. But $U \cap K = Q$, so $\sigma|_K(\alpha) \equiv \alpha \pmod{Q}$. Hence, $\sigma|_K \in E(Q \mid q)$. It follows that we have an embedding $E(U \mid q) \hookrightarrow E(Q \mid q) \times \mathrm{Gal}(L/\mathbb{Q})$. Therefore, $e(U \mid q) = |E(U \mid q)|$ divides $|E(Q \mid q)||\mathrm{Gal}(L/\mathbb{Q})| = e^2$. Now $e = e(Q \mid q)$ divides $[K : \mathbb{Q}] = p^m$. It follows that $e(U \mid q)$ is a power of p. Thus, q does not divide $e(U \mid q)$, so by Prop. 5.5.6, $V_1(U \mid q)$ is trivial. We have that $D(U \mid q)/V_1(U \mid q)$ is abelian. By Prop. 5.5.9, $E(U \mid q)/V_1(U \mid q)$ is cyclic. But $V_1(U \mid q)$ is trivial, so $E(U \mid q)/V_1(U \mid q) \cong E(U \mid q)$. Thus, $E(U \mid q)$ is cyclic. Suppose $E(U \mid q) =< \tau >$. Consider the aforementioned embedding $E(U \mid q) \hookrightarrow$

$E(Q \mid q) \times \mathrm{Gal}(L/\mathbb{Q})$. Let $a = |\tau\big|_K|$ and $b = |\tau\big|_L|$. Then $|(\tau\big|_K, \tau\big|_L)| = \mathrm{lcm}(a,b)$. Since $a \Big| |E(Q \mid q)| = e$ and $b \Big| |\mathrm{Gal}(L/\mathbb{Q})| = e$, we have that $\mathrm{lcm}(a,b) \Big| e$. But $\mathrm{lcm}(a,b) = |(\tau\big|_K, \tau\big|_L)| = |\tau| = e(U \mid q)$. Thus, $e(U \mid q)$ divides e. Now $e(U \mid q) = e(U \mid Q)e(Q \mid q)$, so $e = e(Q \mid q)$ divides $e(U \mid q)$. It follows that $[KL : K'] = e(U \mid q) = e$.

We have that $[KL : \mathbb{Q}]$ divides $[K : \mathbb{Q}][L : \mathbb{Q}] = ep^m$. Since e divides p^m, it follows that $[KL : \mathbb{Q}]$ is a power of p. Therefore, $[K' : \mathbb{Q}]$ is a power of p, say p^k. We have that $ep^k = [KL : K'][K' : \mathbb{Q}] = [KL : \mathbb{Q}]$ which divides ep^m. Therefore, we must have that $k \leq m$. This establishes (2).

We have that $e(U \mid q) = e(U \mid U \cap L)e(U \cap L \mid q)$. Since q is totally ramified in L, $e(U \cap L \mid q) = [L : \mathbb{Q}] = e$. As we just showed, $e(U \mid q) = e$. It follows that $e(U \mid U \cap L) = 1$. Thus, U is unramified over L. Similarly, $e(U \mid q) = e(U \mid U \cap K')e(U \cap K' \mid q)$. We have that q is unramified in K', so $e(U \cap K' \mid q) = 1$. Thus,

$$e(U \mid U \cap K') = e(U \mid q) = |E(U \mid q)| = [KL : (KL)^{E(U \mid q)}] = [KL : K'].$$

Thus, U is totally ramified over K'.

We claim that $K'L = KL$. We have that $K' \subseteq KL$ and $L \subseteq KL$, so $K'L \subseteq KL$. Since U is totally ramified over K', it follows that U is totally ramified over $K'L$. Since U is unramified over L, it follows that U is unramified over $K'L$. Thus, $[KL : K'L] = e(U \mid U \cap K'L) = 1$, so $K'L = KL$.

Supposing K' is contained in the d-th cyclotomic field where q does not divide d, then

$$K \subseteq KL = K'L \subseteq \mathbb{Q}(\omega_d)\mathbb{Q}(\omega_q) = \mathbb{Q}(\omega_{dq}).$$

This establishes (3). □

Proposition 6.3.2. *Suppose K is an abelian extension of $\mathbb{Q}$ with prime power degree p^m. Let q_1, ..., q_t be the primes different from p that are ramified in $R = \mathcal{O}_K$. If p is not ramified in R, then K is contained in the $q_1...q_t$-th cyclotomic field. If $p = 2$ is ramified in R, then K is contained in the $2^{m+2}q_1...q_t$-th cyclotomic field. Lastly, if p is an odd prime and is ramified in R, then K is contained in the $p^{m+1}q_1...q_t$-th cyclotomic field.*

Proof. We will prove this by induction on t. When $t = 0$, we must have that p is ramified in R by Minkowski's Theorem. Prop. 6.2.1 establishes the result when $p = 2$, while Prop. 6.2.5 establishes the result when p is odd.

Now suppose that the result holds for all $0 \leq k < t$. Applying Lemma 6.3.1 with $q = q_t$, we obtain a field K' with the properties (1)-(3). Property (1) gives us that K' has less than t primes different from p that are ramified in $\mathcal{O}_{K'}$. We will apply the inductive hypothesis to K'.

Suppose first that p is unramified in K. Then p is unramified in K' by (1) of Prop. 6.3.1. Moreover, some subset of the primes q_1,...,q_{t-1} are ramified in K'. Applying the inductive hypothesis, we obtain that K' is contained in the $q_1...q_{t-1}$-th cyclotomic field. Taking $d = q_1...q_{t-1}$ in (3) of Prop. 6.3.1 gives us the desired result. Now suppose p is ramified in K. Regardless of whether p ramifies in K' or not, we have that K' is contained in the $2^{k+2}q_1...q_{t-1}$-th cyclotomic field when $p = 2$ and is contained in the $p^{k+1}q_1...q_{t-1}$-th cyclotomic field when p is odd. By Property (2) of Prop. 6.3.1, K' is contained in the $2^{m+2}q_1...q_{t-1}$-th cyclotomic field when $p = 2$ and is contained in the $p^{m+1}q_1...q_{t-1}$-th cyclotomic field when p is odd. Letting $d = 2^{m+2}q_1...q_{t-1}$ when $p = 2$ and $d = p^{m+1}q_1...q_{t-1}$ when p is odd in (3) of Prop. 6.3.1 gives us the desired result. □

6.4 General Case

Now we are ready to prove the general case of the Kronecker-Weber Theorem.

Lemma 6.4.1. *Every abelian extension of $\mathbb{Q}$ is the composition of abelian extensions of prime power degree.*

Proof. Suppose L is an abelian extension of $\mathbb{Q}$ with Galois group G. Suppose $|G| = p_1^{r_1}...p_k^{r_k}$ is the factorization of $|G|$ into primes. For each p_i, let G_i denote the Sylow p_i-subgroup of G. Since G is abelian, G_i is normal in G and hence is the unique Sylow p_i-subgroup. Then $G \cong G_1 \times ... \times G_k$ by the fundamental theorem of finitely-generated abelian groups. Letting $H_i = G_1 \times ... \times G_{i-1} \times \{1\} \times G_{i+1} \times ... \times G_k$, consider the fixed fields $K_i = L^{H_i}$. Then $\mathrm{Gal}(K_i/\mathbb{Q}) \cong G/H_i \cong G_i$. Hence, K_i is an abelian extension of order $p_i^{r_i}$. We have that $K_1...K_k \subseteq L$. Since for each $i \neq j$, $K_i \cap K_j = \mathbb{Q}$, we have that

$$[K_1...K_k : \mathbb{Q}] = [K_1 : \mathbb{Q}]...[K_k : \mathbb{Q}] = p_1^{r_1}...p_k^{r_k} = [L : \mathbb{Q}].$$

Thus, $K_1...K_k = L$. Therefore, L is the composition of abelian extensions of prime power degree. □

Since every abelian extension of prime power degree is contained in a cyclotomic field, it follows that every abelian extension of $\mathbb{Q}$ is contained in a product of cyclotomic fields. Since a product of cyclotomic fields is a cyclotomic field, the Kronecker-Weber Theorem follows. However, we can say more precisely which cyclotomic field it must be contained in.

Theorem 6.4.2. *Suppose K is an abelian extension of $\mathbb{Q}$ of degree $n = p_1^{m_1}...p_s^{m_s}q_1^{l_1}...q_t^{l_t}$ where each p_i is ramified in $\mathcal{O}_K$ and the q_i are unramified in $\mathcal{O}_K$. Let $n' = p_1^{m_1}...p_s^{m_s}$ and let r denote the product of all primes of $\mathbb{Z}$ which are ramified in $\mathcal{O}_K$, with an extra factor of 2 if 2 is ramified and divides n. Then K is contained in the $n'r$-th cyclotomic field.*

Proof. By Lemma 6.4.1, we may factor $K = K_{p_1^{m_1}}...K_{p_s^{m_s}}K_{q_1^{l_1}}...K_{q_t^{l_t}}$ where $[K_a : \mathbb{Q}] = a$. We have that every prime that is ramified in K must necessarily be ramified in some K_a (otherwise, we may apply Prop. 5.3.2 to obtain a contradiction). Let $u_{i1}, ..., u_{ia_i}$ be the primes not equal to p_i that are ramified in $K_{p_i^{m_i}}$, and let $v_{i1}, ..., v_{ib_i}$ be the primes that are ramified in $K_{q_i^{l_i}}$ (necessarily these primes are not equal to q_i since this would imply q_i is ramified in $K_{q_i^{l_i}}$ and hence K). Let $\omega(d) = \omega_d = e^{2\pi i/d}$. By Prop. 6.3.2, we have that

$$K_{p_i^{m_i}} \subseteq \begin{cases} \mathbb{Q}[\omega(u_{i1}...u_{is_i}p_i^{m_i+1})] & \text{if } p_i \text{ is odd} \\ \mathbb{Q}[\omega(u_{i1}...u_{is_i}2^{m_i+2})] & \text{if } p_i = 2 \end{cases}$$

regardless of whether p_i is ramified in $K_{p_i^{m_i}}$, and

$$K_{q_i^{m_i}} \subseteq \mathbb{Q}(\omega(v_{i1}...v_{is_i}))$$

since q_i is necessarily not ramified in $K_{q_i^{m_i}}$. Suppose that all p_i are odd. Then

$$\begin{aligned}
K &= K_{p_1^{m_1}} \ldots K_{p_s^{m_s}} K_{q_1^{l_1}} \ldots K_{q_t^{l_t}} \\
&\subseteq \prod_{i=1}^{s} \mathbb{Q}(\omega(u_{i1} \ldots u_{ia_i} p_i^{m_i+1})) \prod_{i=1}^{t} \mathbb{Q}(\omega(v_{i1} \ldots v_{ib_i})) \\
&= \prod_{i=1}^{s} \mathbb{Q}(\omega(u_{i1})) \ldots \mathbb{Q}(\omega(u_{ia_i})) \mathbb{Q}(\omega(p_i^{m_i+1})) \prod_{i=1}^{t} \mathbb{Q}(\omega(v_{i1})) \ldots \mathbb{Q}(\omega(v_{ib_i})) \\
&= \prod_{u \text{ ramified in } K, u \neq p_i} \mathbb{Q}(\omega(u)) \prod_{i=1}^{s} \mathbb{Q}(\omega(p_i^{m_i+1})) \\
&= \mathbb{Q}\left(\omega\left(\prod_{u \text{ ramified in } K, u \neq p_i} u \prod_{i=1}^{s} p_i^{m_i+1}\right)\right) \\
&= \mathbb{Q}\left(\omega\left(\left(\prod_{u \text{ ramified in } K} u\right)\left(\prod_{i=1}^{s} p_i^{m_i}\right)\right)\right) \\
&= \mathbb{Q}(\omega(rn')).
\end{aligned}$$

Now suppose that $p_s = 2$. Then

$$\begin{aligned}
K &= K_{p_1^{m_1}} \ldots K_{p_{s-1}^{m_{s-1}}} K_{2^{m_s}} K_{q_1^{l_1}} \ldots K_{q_t^{l_t}} \\
&\subseteq \prod_{i=1}^{s-1} \left(\mathbb{Q}(\omega(u_{i1} \ldots u_{ia_i} p_i^{m_i+1}))\right) \mathbb{Q}(\omega(u_{s1} \ldots u_{sb_s} 2^{m_s+2})) \prod_{i=1}^{t} \mathbb{Q}(\omega(v_{i1} \ldots v_{ib_i})) \\
&= \prod_{u \text{ ramified in } K, u \neq p_i} \mathbb{Q}(\omega(u)) \prod_{i=1}^{s-1} \mathbb{Q}(\omega(p_i^{m_i+1})) \mathbb{Q}(\omega(2^{m_s+2})) \\
&= \mathbb{Q}\left(\omega\left(\prod_{u \text{ ramified in } K, u \neq p_i} u \prod_{i=1}^{s-1} p_i^{m_i+1} 2^{m_s+2}\right)\right) \\
&= \mathbb{Q}\left(\omega\left(\left(2 \prod_{u \text{ ramified in } K} u\right)\left(\prod_{i=1}^{s} p_i^{m_i}\right)\right)\right) \\
&= \mathbb{Q}(\omega(rn'))
\end{aligned}$$

In either case, we have that K is contained in the $n'r$-th cyclotomic field. □

6.5 Examples

Example 6.5.1. Let $f(x) = x^9 - 9x^7 + 27x^5 - 30x^3 + 9x - 1$ and K be the splitting field of f. A computation in Maple gives us that $\mathrm{Gal}(K/\mathbb{Q}) \cong C_9$ is the cyclic group of order 9. Thus, K is an abelian extension of $\mathbb{Q}$. What is the smallest cyclotomic field containing K?

Another computation in Maple gives us that

$$\Delta(f) = 31381059609 = 3^{22}.$$

Let $R = \mathcal{O}_K$. We know that by Prop. 3.3.2 and Prop. 3.3.7 that $\Delta(R)$ divides $\Delta(f) = 3^{22}$. It follows from Theorem 4.4.1 that the only prime of $\mathbb{Z}$ which could ramify in K is 3. Indeed, Minkowski's Theorem implies that 3 must ramify in K. In the notation of Theorem 6.4.2,

$$n = [K : \mathbb{Q}] = |\,\mathrm{Gal}(K/\mathbb{Q})| = 9 = 3^2,$$

$n' = 9$, and $r = 3$. Hence, $n'r = 27$. Therefore K is contained in the 27-th cyclotomic field. Moreover, if $K \subseteq \mathbb{Q}(\omega(m))$ for any integer $m \geq 1$, then

$$K \subseteq \mathbb{Q}(\omega(27)) \cap \mathbb{Q}(\omega(m)) = \mathbb{Q}(\omega(\gcd(27, m))).$$

It follows that the smallest cyclotomic field containing K is either $\mathbb{Q}(\omega(3))$, $\mathbb{Q}(\omega(9))$, or $\mathbb{Q}(\omega(27))$. However, $K \not\subseteq \mathbb{Q}(\omega(9))$ (and hence $K \not\subseteq \mathbb{Q}(\omega(3))$) since

$$[\mathbb{Q}(\omega(9)) : \mathbb{Q}] = 6 < 9 = [K : \mathbb{Q}].$$

It follows that $\mathbb{Q}(\omega(27))$ is the smallest cyclotomic field containing K.

Example 6.5.2. Let $h(x) = x^9 - 30x^7 + 24x^6 + 237x^5 - 228x^4 - 577x^3 + 384x^2 + 432x + 64$, and let M be the splitting field of h. A computation in Maple gives us that $\mathrm{Gal}(K/\mathbb{Q}) \cong C_3 \times C_3$. Thus, M is an abelian extension of $\mathbb{Q}$. Again, we ask what is the smallest cyclotomic field containing M?

Another computation in Maple gives us that

$$\Delta(h) = 2^{18} \cdot 3^{12} \cdot 7^6 \cdot 503^2 \cdot 2267^2.$$

Let $R = \mathcal{O}_M$. We know that by Prop. 3.3.2 and Prop. 3.3.7 that $\Delta(R)$ divides $\Delta(h)$. It follows from Theorem 4.4.1 that the only primes of $\mathbb{Z}$ which could ramify in M are 2, 3, 7, 503, and 2267. We have that

$$n = [M : \mathbb{Q}] = |\,\mathrm{Gal}(M/\mathbb{Q})| = 9 = 3^2.$$

Using the notation of Theorem 6.4.2, we have that $n' \leq 9$ and $r \leq 2 \cdot 3 \cdot 7 \cdot 503 \cdot 2267$. It follows that M is contained in the $nr' \leq 431,033,778$-th cyclotomic field. But is this the smallest cyclotomic field containing M? Of course, we could always try to determine which of the primes 2, 3, 7, 503, and 2267 actually ramify in M which would give us a better bound. It turns out that 3 and 7 are the only primes that ramify in M, for reasons which we will get to in a moment. This gives us that $n' = 9$ and $r = 3 \cdot 7 = 21$, so Theorem 6.4.2 gives us that M is contained in the 189-th cyclotomic field. Although this is a huge improvement, it is still not the smallest cyclotomic field containing M.

Let $f(x) = x^3 - 3x + 1$ and $g(x) = x^3 - 7x + 7$, and let K and L be the respective splitting fields of f and g. A computation in Maple gives us that $\mathrm{Gal}(K/\mathbb{Q}) \cong C_3$ and $\mathrm{Gal}(L/\mathbb{Q}) \cong C_3$. Let α be a root of f and β be a root of g. Then h is the minimal polynomial of $\alpha + \beta$ (indeed, this is how h was constructed...). It follows that $M \subseteq KL$, and since the degrees of the two fields over $\mathbb{Q}$ are equal, we must have that $M = KL$. We will consider what are the smallest cyclotomic fields containing K and L. We have that

$$\Delta(f) = 3^4 \quad \Delta(g) = 7^2.$$

It follows that the only prime which can ramify in K is 3, and Minkowski's Theorem gives us that 3 must ramify in K. Similarly, we obtain that 7 is the only prime which ramifies in L. Consequently, 3 and 7 must also ramify in M, and Prop. 5.3.2 gives us that no other primes of $\mathbb{Z}$ ramify in $KL = M$. For K, we have that $n' = 3$ and $r = 3$, so K is contained in the 9-th cyclotomic field. For L, we have that $n' = 1$ and $r = 7$, so L is contained in the 7-th cyclotomic field. We must have that $\mathbb{Q}(\omega(7))$ is the smallest cyclotomic field containing L since the only other cyclotomic field contained in $\mathbb{Q}(\omega(7))$ is $\mathbb{Q}$. Moreover, we have that $\mathbb{Q}(\omega(9))$ contains a unique subfield of degree 3 over $\mathbb{Q}$, namely $\mathbb{Q}(\omega(3))$. It follows that $K = \mathbb{Q}(\omega(3))$. Therefore,

$$M = KL \subseteq \mathbb{Q}(\omega(3))\mathbb{Q}(\omega(7)) = \mathbb{Q}(\omega(21)).$$

Since $\mathbb{Q}(\omega(21))$ is the smallest cyclotomic field where 3 and 7 ramify (from Theorem 5.4.1), it follows that $\mathbb{Q}(\omega(21))$ is the smallest cyclotomic field containing M.

The previous two examples illustrated two important points. The first point is that given an abelian extension K over $\mathbb{Q}$, using nothing more than the discriminant and the

degree of K over $\mathbb{Q}$, we can use Theorem 6.4.2 to obtain a cyclotomic field containing K. In the first example, this gave us the smallest cyclotomic field containing K, while in the second we obtained a cyclotomic field that was far from optimal. The second point is even with knowledge of which integer primes ramify in K, Theorem 6.4.2 does not generally give the smallest cyclotomic field containing K. In the second example, by factoring our field into subfields, we were able to determine that the smallest cyclotomic field is the 21-st, while Theorem 6.4.2 only told us it was contained in the 189-th cyclotomic field.

Lastly, one might wonder if the Kronecker-Weber Theorem is true if we start with a base field K different from $\mathbb{Q}$. That is, if L is a finite, abelian extension of K, is it true that $L \subseteq K(\omega(m))$ for some positive integer m? The answer is no as the next example illustrates.

Example 6.5.3. Let $K = \mathbb{Q}(i) = \mathbb{Q}(\omega(4))$ and let $L = K(\sqrt[4]{2})$. We have that L is the splitting field of $f(x) = x^4 - 2$, so L is normal over $\mathbb{Q}$, and hence L must be normal over K. Moreover, $\mathrm{Gal}(L/K) \cong C_4$, so L is an abelian extension of K. Now for any positive integer m, we have that $K(\omega(m)) = \mathbb{Q}(\omega(\mathrm{lcm}(4, m))$. Hence, if $L \subseteq K(\omega(m))$ for some integer m, then L is contained in a cyclotomic field. Consequently, L must be an abelian extension of $\mathbb{Q}$. However, $\mathrm{Gal}(L/\mathbb{Q}) \cong D_8$ is the dihedral group of order 8. Thus, L is not an abelian extension of $\mathbb{Q}$. Consequently, L is not contained in $K(\omega(m))$ for any positive integer m.

An open problem in mathematics is to determine a generalization of the Kronecker-Weber Theorem for arbitrary base fields K. This is Hilbert's Twelfth Problem. As the above example illustrates, finite, abelian extensions of K need not be contained in cyclotomic extensions of K. There is a generalization when K is an imaginary quadratic field $\mathbb{Q}(\sqrt{-m})$ where m is a squarefree positive integer. However, it is another class of fields, not cyclotomic fields, that contain all finite, abelian extensions of $\mathbb{Q}(\sqrt{-m})$. These two examples suggest that there should be some sort of generalization of the Kronecker-Weber Theorem, although what that generalization is, if it exists, is still unknown.

Bibliography

[1] Keith Conrad. History of class field theory. Expository papers/Lecture notes. Available at http://www.math.uconn.edu/~kconrad/blurbs/gradnumthy/cfthistory.pdf.

[2] Daniel A. Marcus. *Number Fields.* Springer-Verlag, 1977.

[3] David S. Dummit and Richard M. Foote. *Abstract Algebra.* John Wiley and Sons, Inc., third edition, 2004.

[4] Ian Stewart. *Galois Theory.* Chapman & Hall/CRC, third edition, 2004.

[5] Keith Conrad. The different ideal. Expository papers/Lecture notes. Available at http://www.math.uconn.edu/~kconrad/blurbs/gradnumthy/different.pdf.